

2250190266

STATE OF SOUTH DAKOTA
VENDOR CONTRACT
BETWEEN

Accela
2633 Camino Ramon Ste. 500
San Ramon, CA 94583
(925) 659-3200

Referred to as "Vendor"

South Dakota Department of Health
600 East Capitol Avenue
Pierre, SD 57501-2536
(605) 773-3361

Referred to as "State"

State and Vendor hereby enter into a contract for project based professional services and modifiable off the shelf software.

I. VENDOR

- A. The term of this Contract shall begin September 29, 2021 and end September 28, 2026. The State of South Dakota retains three additional options to extend the contract period by one year each.
- B. Vendor is not a full or part-time employee of State or any agency of the state of South Dakota.
- C. Vendor, as an independent contractor, is solely responsible for the withholding and payment of applicable income and Social Security taxes due and owing from money received under this contract.
- D. Vendor will not be utilizing any equipment, supplies or facilities owned by the state of South Dakota.
- E. Vendor will not purchase capital assets or equipment using State funds.
- F. Vendor agrees to provide the Subscription Services as outlined in the Accela Subscription Services Agreement, incorporated herein as Exhibit A-1, and complete the activities outlined in the Accela Statement of Work, incorporated herein as Exhibit A-2.
- G. **INSURANCE:** Vendor agrees, at its sole cost and expense, to maintain the following insurance:
 - 1. Commercial General Liability Insurance:
Vendor shall maintain occurrence based commercial general liability insurance or equivalent form with a limit of not less than \$1,000,000 each occurrence. If such insurance contains a general aggregate limit it shall apply separately to this contract or be no less than two times the occurrence limit.
 - 2. Professional and Cyber Liability Insurance:

Vendor shall procure and maintain professional and cyber liability insurance with liability limits in the amount of \$10 million dollars to protect State data the Vendor receives as part of the project covered by this agreement including State data that may reside on devices,

including laptops and smart phones, utilized by Vendor employees, whether the device is owned by the employee or the Vendor. If the Vendor has a contract with a third-party to host any State data the Vendor receives as part of the project under this agreement, then the Vendor shall include a requirement for cyber liability insurance as part of the contract between the Vendor and the third-party hosting the data in question. The third-party cyber liability insurance coverage will include State data that resides on devices, including laptops and smart phones, utilized by third-party employees, whether the device is owned by the employee or the third-party Vendor. The cyber liability insurance shall cover expenses related to the management of a data breach incident, the investigation, recovery and restoration of lost data, data subject notification, call management, credit checking for data subjects, legal costs, and regulatory fines. Before beginning work under this Agreement, the Vendor shall furnish the State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Agreement. The insurance will stay in effect for 2 years after the work covered by this agreement is completed.

3. Business Automobile Liability Insurance:

Vendor shall maintain business automobile liability insurance or equivalent form with a limit of not less than \$1,000,000 each accident. Such insurance shall include coverage for owned, hired and non-owned vehicles as applicable.

4. Worker's Compensation Insurance:

Vendor shall procure and maintain workers' compensation and employers' liability insurance as required by South Dakota law.

5. Certificates of Insurance:

Before beginning work under this Contract, Vendor shall furnish State with properly executed Certificates of Insurance which shall clearly evidence all insurance required in this Contract. In the event of issuance of a new policy, cancellation or nonrenewal of the policy, Vendor agrees to provide immediate notice to the State and provide a new certificate of insurance showing continuous coverage in the amounts required.

- H. Subject to the Limitation of Liability in Exhibit A-1, Vendor agrees to indemnify and hold the State of South Dakota, its officers, agents and employees, harmless from and against any and all actions, suits, damages, liability or other proceedings that may arise as a result of performing services hereunder. This section does not require Vendor to be responsible for or defend against claims or damages arising solely from acts or omissions of the State, its officers, agents or employees.

II. STATE

- A. State will pay, upon the State's satisfaction that the payments are in accordance with all items of the contract, up to \$880,246.93. Expenditure claims are required prior to the initiation of any and all payments. Expenditure claim documentation may include: invoices for reimbursement; receipts of any goods or services purchased; purchase orders for supplies, equipment, etc.; and/or itemized budget details indicating how and the timeframe in which the funds will be used.
- B. State will not pay Vendor expenses as a separate item.
- C. TOTAL CONTRACT AMOUNT (Not to Exceed) \$880,246.93. Payment will be made consistent with SDCL Ch. 5-26.

- D. State will not be held liable for reimbursement of amounts shown on an itemized billing if not received within 30 calendar days from the close of the month being reported. However, the final invoice of the State of South Dakota fiscal year, ending every year on June 30th, shall be submitted no later than June 9th so payment may be made in the same Fiscal Year as the services are provided.
- E. State agrees to complete the activities outlined in the Accela Statement of Work, which is incorporated as Exhibit A.
- F. Pursuant to South Dakota Codified Law 1-33-44, the Bureau of Information and Telecommunications ("BIT") oversees the acquisition of office systems technology, software and services; telecommunication equipment, software and services; and data processing equipment, software, and services for departments, agencies, commissions, institutions and other units of state government. BIT requires the contract provisions which are attached to this Agreement as Exhibit C and incorporated into this Agreement by reference. It is understood and agreed to by all parties that BIT, as the State's technology governing organization, has reviewed only Exhibit C of this agreement. Before renewal of this Agreement BIT must review and approve Exhibit C as still being current. BIT's evaluation of Exhibit C will be based on changes in the IT security or regulatory requirements. Changes to Exhibit C must be approved in writing by all parties before they go into effect and a renewal of this Agreement is possible. The most current version of the State's Information Technology Security Policy will also be provided to the Vendor with the understanding that the Vendor will adhere to the most current State IT security policies.
- G. Vendor agrees to the terms of the Security Acknowledgement form, incorporated into this agreement as Exhibit D.

III. OTHER PROVISIONS

- A. **CHOICE OF LAW AND FORUM.** The terms and conditions of this contract are subject to and will be construed under the laws of the State of South Dakota. The parties further agree that any dispute arising from the terms and conditions of this contract, which cannot be resolved by mutual agreement, will be tried in the Sixth Judicial Circuit Court, Hughes County, South Dakota.
- B. **INTEGRATION.** This contract is a complete version of the entire agreement between the parties with respect to the subject matter within this contract and supersedes all prior or contemporaneous written or oral understandings, agreements and communications between them with respect to such subject matter. This contract may be modified or amended only by a writing signed by both parties.
- C. **TERMINATION:** This contract may be terminated by either party hereto upon thirty (30) days written notice, and may be terminated by State for cause at any time, with or without notice.
- D. **NOTICE:** Any notice or other communication required under this contract shall be in writing and sent to the address set forth above. Notices shall be given by and to the State Contact Person on behalf of State, and by and to the Vendor Contact Person on behalf of Vendor, or such authorized designees as either party may from time to time designate in writing. Notices or communications to or between the parties shall be deemed to have been delivered when mailed by first class mail, provided that notice of default or termination shall be sent by registered or certified mail, or, if personally delivered, when received by such party.

- E. **ASSURANCES:** The Vendor agrees to abide by all applicable provisions of the following assurances: Lobbying Activity, Byrd Anti Lobbying Amendment (31 USC 1352), Drug-Free Workplace, Executive Order 11246 Equal Employment Opportunity, Title VI of the Civil Rights Act of 1964, Title VIII of the Civil Rights Act of 1968, Section 504 of the Rehabilitation Act of 1973, Title IX of the Education Amendments of 1972, Drug Abuse Office and Treatment Act of 1972, Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970, Age Discrimination Act of 1975, Americans with Disabilities Act of 1990, Pro-Children Act of 1994, Hatch Act, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Clean Air Act, Federal Water Pollution Control Act, Charitable Choice Provisions and Regulations, Equal Treatment for Faith-Based Religions at Title 28 Code of Federal Regulations Part 38, the Violence Against Women Reauthorization Act of 2013, American Recovery and Reinvestment Act of 2009, and Section 106 (g) of the Trafficking Victims Protection Act of 2002, as amended (22 U.S.C. 7104) as applicable.
- F. **RESTRICTION OF BOYCOTT OF ISRAEL:** Pursuant Executive Order 2021-01, for contractors, vendors, supplies, or subcontracts with five (5) or more employees who enter into a contract with the State of South Dakota that involves the expenditure of one hundred thousand dollars (\$100,000) or more, by signing this contract Vendor certifies and agrees that it has not refused to transact business activities, have not terminated business activities, and have not taken other similar actions intended to limit its commercial relations, related to the subject matter of the contract, with a person or entity that is either the State of Israel, or a company doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel to do business, or doing business in the State of Israel, with the specific intent to accomplish a boycott or divestment of Israel in a discriminatory manner. It is understood and agreed that, if this certification is false, such false certification will constitute grounds for State to terminate this contract. Vendor further agrees to provide immediate written notice to State if during the term of the contract it no longer complies with this certification, and agrees such noncompliance may be grounds for contract termination.
- G. **CERTIFICATION REGARDING DEBARMENT, SUSPENSION, INELIGIBILITY, AND VOLUNTARY EXCLUSION:**
Vendor agrees that neither Vendor, nor any of Vendor's principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions by any Federal department or agency. Vendor will provide immediate written notice to the Department of Health, Division of Administration (600 East Capitol Avenue, Pierre, SD 57501 (605) 773-3361), if Vendor, or any of Vendor's principals, becomes debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in transactions involving Federal funding. Vendor further agrees that if this contract involves federal funds or federally mandated compliance, then Vendor is in compliance with all applicable regulations pursuant to Executive Order 12549, including Debarment and Suspension and Participants' Responsibilities, 29 C.F.R. § 98.510 (1990).
- H. **FUNDING TERMINATION:** This contract depends upon the continued availability of appropriated funds and expenditure authority from Congress, the Legislature or the Executive Branch for this purpose. This contract will be terminated for cause by State if Congress, the Legislature or Executive Branch fails to appropriate funds, terminates funding or does not grant expenditure authority. Funding termination is not a default by State nor does it give rise to a claim against State.
- I. **NONASSIGNMENT/SUBCONTRACTING:** Except in the event of an acquisition or change in control, Vendor shall not assign this contract, or any portion thereof, without the prior written

consent of State. Vendor's assignment or attempted assignment of this contract in violation of this Section, or any portion thereof, constitutes a material breach of contract. The Vendor may not use subcontractors to perform the services described herein without the express prior written consent of State. Vendor will include provisions in its subcontracts requiring its subcontractors to comply with the applicable provisions of this Agreement, to indemnify the State, and to provide insurance coverage in a manner consistent with this Agreement. Vendor will cause its subcontractors, agents, and employees to comply with applicable federal, state and local laws, regulations, ordinances, guidelines, permits and requirements and will adopt such review and inspection procedures as are necessary to assure such compliance.

- J. **FEDERAL AND STATE LAWS:** Vendor agrees that it will comply with all federal and state laws, rules and regulations as they may apply to the provision of services pursuant to this contract, including the Americans with Disabilities Act (ADA) of 1990, 42 U.S.C. §§ 12101-12213, and any amendment thereto, Section 306 of the Clean Air Act, and Section 508 of the Clean Water Act. Both parties further agree to provide services covered by this contract without regard to race, color, national origin, sex, age or disability as prohibited by state or federal law.

- K. **RESERVED .**

- L. **REPORTING OF PERSONAL INJURIES AND/OR PROPERTY DAMAGE:** Vendor agrees to report promptly to State any event encountered in the course of performance of this contract which results in injury to the person or property of third parties, or which may otherwise subject Vendor or State to liability. Reporting to State under this section does not satisfy Vendor's obligation to report any event to law enforcement or other entities as required by law.

- M. **SEVERABILITY:** In the event that any term or provision of this contract shall violate any applicable law, such provision does not invalidate any other provision hereof.

- N. **AUDIT REQUIREMENTS:**

(EXPENDING \$750,000 OR MORE)

A nonprofit subrecipient, (as well as profit hospitals) (Vendor), expending \$750,000 or more in one year in Federal awards, must have an annual audit made in accordance with 2 CFR Chapter I, Chapter II, Part 200, et al. Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards.

All audits must be conducted by an auditor approved by the Auditor General to perform the audit. Approval may be obtained by forwarding a copy of the audit engagement letter to the Department of Legislative Audit, 427 South Chapelle, c/o 500 East Capitol, Pierre, SD 57501-5070. On continuing engagements, the Auditor General's approval should be obtained annually. The auditor must follow the Auditor General's guidelines when conducting the audit. The draft audit report must be submitted to the Auditor General for approval prior to issuing the final report. The auditor must file the requested copies of the final audit report with the Auditor General. Audits shall be completed and filed with granting agencies by the end of the ninth month following the end of the fiscal year being audited or 30 days after receipt of the auditor's report, whichever is earlier. If it appears that a required audit cannot be completed by the end of the ninth month following your fiscal year, you must request an extension from the federal agency for which the majority of federal expenditures relates.

Failure to complete audit(s) as required will result in the disallowance of audit costs as direct or indirect charges to programs. Additionally, a percentage of awards may be withheld, overhead

costs may be disallowed, and/or awards may be suspended, until the audit is completed satisfactorily.

- O. **FORCE MAJEURE:** Neither Vendor nor State shall be liable to the other for any delay in, or failure of performance of, any covenant or promise contained in this contract, nor shall any delay or failure constitute default or give rise to any liability for damages if, and only to the extent that, such delay or failure is caused by "force majeure". As used in this contract, "force majeure" means acts of God, acts of the public enemy, acts of the State and any governmental entity in its sovereign capacity, fires, floods, epidemics, quarantine restrictions, strikes or other labor disputes, freight embargoes, or unusually severe weather.
- P. **CONTRACT ORIGINAL AND COPIES:** An original of this contract will be retained by the State Auditor's Office. A photocopy will be on file with the South Dakota Department of Health and a second original will be sent to Vendor.
- Q. **RECORD RETENTION/EXAMINATION:** Vendor agrees to maintain all records that are pertinent to this contract and retain them for a period of three years following final payment against the contract. State agrees to assume responsibility for these items after that time period. These records shall be subject at all reasonable times for inspection, review or audit by State, other personnel duly authorized by State, and federal officials so authorized by law.
- R. **LICENSING AND COMPLIANCE:** The Vendor agrees to comply in full with all licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance in which the service and/or care is provided for the duration of this agreement. The Vendor will maintain effective internal controls in managing the federal award. Liability resulting from noncompliance with licensing and other standards required by Federal, State, County, City or Tribal statute, regulation or ordinance or through the Vendor's failure to ensure the safety of all individuals served is assumed entirely by the Vendor.
- S. **RESERVED .**
- T. **CONFLICT OF INTEREST:** Provider agrees to establish safeguards to prohibit employees or other persons from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain as contemplated by SDCL 5-18A-17 through 5-18A-17.6. Any potential conflict of interest must be disclosed in writing. In the event of a conflict of interest, the Provider expressly agrees to be bound by the conflict resolution process set forth in SDCL 5-18A-17 through 5-18A-17.6.
- U. **RECYCLING.** State strongly encourages Vendor to establish a recycling program to help preserve our natural resources and reduce the need for additional landfill space.

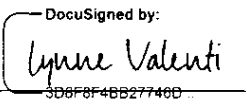
Signature page to follow.

In WITNESS WHEREOF, the parties have indicated their acceptance of the terms of this Agreement by their signatures below.

South Dakota Department of Health

Lynn Valenti

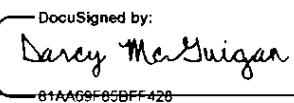
Deputy Secretary / Division Director of Healthcare Access & Quality and Health Protection

By: 
 9/30/2021

Date: _____

Darcy McGuigan

Director, Division of Finance

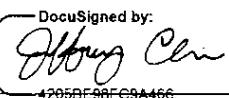
By: 
 9/30/2021

Date: _____

South Dakota Bureau of Information and Telecommunications *(approval as to Exhibit C only)*

Jeff Clines

Commissioner

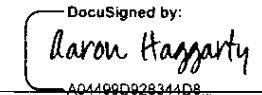
By: 
 10/1/2021

Date: _____

Accela, Inc.

Aaron Haggarty

Chief Legal Officer

By: 
 10/1/2021

Date: _____

**BUSINESS ASSOCIATE AGREEMENT BETWEEN:
THE SOUTH DAKOTA DEPARTMENT OF HEALTH, AND CLOUDPWR.**

This Business Associate Agreement (hereinafter may be referred to as "BAA") is made and entered into by and between the South Dakota Department of Health (hereinafter referred to as "DOH") and CloudPWR (hereinafter referred to as "the vendor"), for the purpose of sharing information between one another regarding medical records of patients to provide for legal, investigative, and other services on behalf of the State of South Dakota.

DOH, and CloudPWR hereby enter into a Business Associate Agreement in consideration of and pursuant to the terms and conditions set forth herein.

1. DOH is a state agency of the State of South Dakota and is governed by the statutes and administrative rules of the same.
2. CloudPWR is a private company contracted by DOH to provide and implement the Modifiable Off-The-Shelf Software (MOTS) that serves as the state's medical marijuana patient registry, verification, and medical marijuana business licensing system.
3. This Business Associate Agreement will be effective immediately upon the signing of this document by authorized representatives of all parties.

I. CLOUDPWR RESPONSIBILITIES

CloudPWR is a Business Associate of the Department of Health pursuant to requirements of the Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act §§ 13400-13424, 42 U.S.C. §§ 17921-17954 (2009). State's Administrative Policies and Procedures Statement No. 24, as modified from time to time during the term of this agreement, is incorporated by reference and made a part of this agreement as if fully set forth herein.

I. Privacy and Security Requirements

1. As a Business Associate, the vendor agrees:
 - a. to use or disclose any Protected Health Information (PHI) solely:
 - i. to meet its obligations in this and any other agreements with State;
 - ii. as required by applicable law, rule or regulation; and
 - iii. as permitted by HIPAA, and any amendments to HIPAA, and subject in particular to limits set forth in 45 CFR § 164.514 (e) (2) (limited data sets) and 45 CFR § 164.502(b) (minimum necessary disclosure requirements);
 - b. to return or destroy all PHI received from, created, or received on behalf of State, at termination of this agreement, or upon request of the DOH, whichever occurs first, or, if such return or destruction is not

feasible, to extend the protections of this agreement to the information and limit further uses and disclosures of such PHI;

- c. to ensure that its agents, including a subcontractor, to whom it provides PHI received from or created by the vendor on behalf of State, agrees to the same restrictions and conditions applicable to the vendor, and agrees to implement reasonable and appropriate safeguards to protect all Electronic Protected Health Information (EPHI). the vendor also agrees to take reasonable steps to ensure that its employees' actions or omissions do not cause a breach of the terms of this agreement;
 - d. to notify State of any discovery or a breach of unsecured PHI as defined in the HITECH Act or accompanying regulations pursuant to the terms of 45 CFR § 164.410 and cooperate in State's breach analysis procedures, if requested. A breach shall be treated as discovered by the vendor as of the first day on which such breach is known, or, by exercising reasonable diligence, would have been known, and requires notification to State without unreasonable delay and in no event later than thirty (30) calendar days after discovery of the breach. Such notification will contain the elements required in 45 CFR § 164.410; and
 - e. to comply with all requirements pursuant to the HITECH Act and its implementing regulations, and all additional applicable requirements of the Privacy Rule, including those contained in 45 CFR §§ 164.502(e) and 164.504(e)(1)(ii). The vendor will not directly or indirectly receive remuneration in exchange for any PHI, subject to the exceptions contained in the HITECH Act and without a valid authorization from the applicable individual. The vendor will not engage in any communication which might be deemed to be "marketing" under the HITECH Act, and will comply with all applicable security requirements in 45 CFR §§ 164.308, 164.310, 164.312, and 164.316.
2. Notwithstanding the prohibitions set forth in this agreement, the vendor may use and disclose PHI if necessary, for its proper management and administration or to carry out its legal responsibilities, provided the following requirements are met:
- a. the disclosure is required by law; or
 - b. reasonable assurances are obtained from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed. Such person shall notify the vendor of any instances of which it is aware in which the confidentiality of the information has been breached.
3. Availability of PHI

The vendor further agrees:

- a. to comply with any request for restrictions on certain disclosures of PHI pursuant to 45 CFR § 164.522, as agreed by State and with notice to Claims Associates
- b. to make PHI available for purposes of accounting of disclosures, as required by 45 CFR § 164.528 and Section 13405(c)(3) of the HITECH Act; and
- c. to cooperate in providing any accounting required on a timely basis.

4. Termination

- a. Termination for convenience. Either party may terminate this contract upon 180 days written notice to the other.
- b. Termination for Cause. The vendor authorizes termination of this contract by DOH, if DOH determines that the vendor has violated a material term of the contract.

5. Miscellaneous

- a. Vendor agrees to indemnify and hold the State, its officers, agents, and employees, harmless from and against any and all actions, suits, damages, liability, or other proceedings which may arise as the result of performing services hereunder. This section does not require the Vendor to be responsible for or defend against claims or damages arising solely from the errors or omissions of the State, its officers, agents, or employees; or from the errors or omissions of third parties that are not officers, employees or agents of the Vendor, unless such errors or omissions resulted from the acts or omissions of the Vendor. Nothing in this Agreement is intended to impair the insurance coverage of the Vendor or any subrogation rights of the Vendor's insurers.
- b. This Agreement may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. The parties agree to take such action as is necessary to amend this Agreement periodically as is necessary to achieve or maintain compliance with the requirements of the HIPAA Rules and any other applicable law.
- c. Any reference herein in this Agreement to a federal regulatory section within the Code of Federal Regulations or a HIPAA rule means the section in effect or as subsequently updated, amended, or modified.
- d. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA rules.

- e. In the event of a conflict in or between the terms of this Business Associate Agreement any interpretation shall ensure compliance with the HIPAA Rules.
- f. Any notices hereunder shall be in writing and addressed as follows:

If to the Business Associate/Vendor:

CloudPWR
PO Box 7906
Tacoma, WA. 98417
Attention: Shadrach White

If to Covered Entity/State:

South Dakota Department of Health
Hayes Building
600 East Capitol
Pierre, SD 57501
Attention: Justin Williams

In Witness Whereof, the parties signify their agreement by the signatures affixed below.

FOR BUSINESS ASSOCIATE/VENDOR – CloudPWR

By:  9/30/2021 | 9:47 AM PDT
F18831018F3A423
Date

Name:

Title:

FOR COVERED ENTITY/STATE - South Dakota State Department of Health

By:  9/30/2021
3D8F8F48B27746D
Date

Name: Lynne Valenti

Title: Deputy Secretary/Division Director of Healthcare Access & Quality and Health Protection
South Dakota Department of Health



ACCELA SUBSCRIPTION SERVICES AGREEMENT

This Accela Subscription Services Agreement (this "**Agreement**") is entered into as of the date of the applicable Order, as defined below, that incorporates these terms (the "**Effective Date**") by and between Accela, Inc. and the entity identified in such Order ("**Customer**").

1. DEFINITIONS.

1.1 "**Accela System**" means the information technology infrastructure used by or on behalf of Accela in performing the Subscriptions Services, including all computers, software (including but not limited to Accela Software), hardware, databases, electronic systems (including database management systems), and networks, whether operated directly by Accela or its third party suppliers.

1.2 "**Aggregate Data**" means data and information related to Customer's use of the Subscription Services, including anonymized analysis of all data processed in the Subscription Services, that is used by Accela in an aggregate and anonymized manner, including compiling statistical and performance information related to the provision and operation of the Services.

1.3 "**Authorized User**" means one named employee, contractor or agent of Customer (each identified by a unique email address) for whom Customer has purchased a subscription to the Subscription Services and who is authorized by Customer to access and use the Services under the rights granted to Customer pursuant to this Agreement.

1.4 "**Consulting Services**" means packaged or time and materials consulting, review, training or other services (but excluding Subscription and Support Services) delivered by Accela to Customer pursuant an Order. The current Consulting Services Policy is available at www.accela.com/terms/.

1.5 "**Customer Data**" means the content, materials, and data that Customer, Authorized Users, and External Users enter into the Subscription Services. Customer Data does not include any component of the Subscription Services, material provided by or on behalf of Accela, or Aggregate Data.

1.6 "**Documentation**" means the then-current technical and functional user documentation in any form made generally available by Accela for the Subscription Services.

1.7 "**External Users**" means third party users of the Subscription Services that access the public-facing interfaces of the Subscription Services to submit queries and requests to facilitate communications between such third party and Customer.

1.8 "**Intellectual Property Rights**" means any patent rights (including, without limitation, patent applications and disclosures), copyrights, trade secrets, know-how, and any other intellectual property rights, in all cases whether or not registered or registrable and recognized in any country or jurisdiction in the world.

1.9 "**Order**" means an Accela order form or other mutually acceptable document fully executed between Customer and Accela that incorporates this Agreement.

1.10 "**Service Availability Policy**" means the Service Availability and Security Policy located at www.accela.com/terms/.

1.11 "**Subscription Services**" means the civic administration services, comprised of the Accela System, Software, and Support Services, to which Customer may license access to in accordance with the terms herein.



1.12 “**Software**” means any licensed software (including client software for Authorized Users’ devices) and Documentation that Accela uses or makes available as part of the Subscription Services.

1.13 “**Support Services**” means those technical and help services provided by Accela in accordance with the Software Support Services Policies (SaaS) located at www.accela.com/terms/.

1.14 “**Subscription Period**” means the duration of Customer’s authorized use of the Subscription Services as designated in the Order.

2. USAGE AND ACCESS RIGHTS.

2.1 Right to Access. Subject to the terms and conditions of this Agreement, Accela hereby grants to Customer a limited, non-exclusive, non-transferable right and license during the Subscription Period, to permit: (i) Authorized Users to access and use the internal and administrative interfaces of the Subscription Services in accordance with the Documentation to support Customer’s internal business purposes and (ii) its External Users the ability to access and use the publicly available interfaces to submit requests and information to Customer. Each instance of the Subscription Service shall be provisioned with the amount of storage set forth in the Order and additional storage may be purchased at the then-current rates.

2.2 Support Services & Service Availability. During the Subscription Period, Accela shall provide to Customer the Support Services specified in the Order and shall make all commercially reasonable efforts to attain the service levels specified in the applicable policies. The remedies set forth in the Support Services and Service Availability Policy are the sole and exclusive remedies for any breach of the service levels. Customer grants Accela a royalty-free, worldwide, transferable, sub- licensable, irrevocable, perpetual license to use or incorporate into its software or services any suggestions or other feedback provided by Customer or Authorized Users relating to the operation or features of the Subscription Services.

2.3 Purchasing Consulting Services. Customer may purchase Consulting Services from Accela by executing an Order for such services. All prices are exclusive of travel and expenses, which will be invoiced at actual cost, without markup, and will comply with the Consulting Services Policy located at www.accela.com/terms/ or as otherwise agreed in the applicable Order. If applicable, one Consulting Services day shall be equal to eight (8) hours.

2.4 Restrictions on Use. Customer shall not, and shall not permit others to: (i) use or access the Subscription Services in any manner except as expressly permitted by the Agreement, including but not limited to, in a manner that circumvents contractual usage restrictions set forth in this Agreement; (ii) license, sub-license, sell, re-sell, rent, lease, transfer, distribute, time share or otherwise make any portion of the Subscription Services available for access by third parties except as otherwise expressly provided herein; (iii) use the Subscription Service in a way that: (a) violates or infringes upon the rights of a third party; or (b) stores or transmits libelous, tortious, or otherwise unlawful material or malicious code or viruses; (iv) create derivative works, reverse engineer, decompile, disassemble, copy, or otherwise attempt to derive source code or other trade secrets from or about any of the Subscription Services (except to and only to the extent such rights are proscribed by law); (v) interfere with or disrupt the security, integrity, operation, or performance of the Subscription Services; (vi) access, use, or provide access or use to the Subscription Services or Documentation for the purposes of competitive analysis or the development, provision, or use of a competing software, SaaS or product or any other purpose that is to Accela’s detriment or commercial disadvantage; (vii) provide access to the Subscription Services to competitors of Accela; (viii) access or use components of the Subscription Service not licensed by Customer; (ix) use or allow the use of the Subscription Services by anyone located in, under the control of, or that is a national or resident of a U.S. embargoed country or territory or by a prohibited end user



under Export Control Laws (as defined in Section 12.3, Compliance with Laws); (x) remove, delete, alter or obscure any trademarks, Documentation, warranties, or disclaimers, or any copyright, trademark, patent or other intellectual property or proprietary rights notices from any Subscription Services; or (xi) access or use the Subscription Services in, or in association with, the design, construction, maintenance, or operation of any hazardous environments, systems or applications, any safety response systems or other safety-critical applications, or any other use or application in which the use or failure of the Subscription Services could lead to personal injury or severe physical or property damage.

2.5 Ownership. Accela retains all Intellectual Property Rights, including all rights, title and license to the Subscription Service, Software, Accela System, Support Services, Consulting Services, and Aggregate Data, any related work product of the foregoing and all derivative works thereof by whomever produced; provided however, that to the extent such materials are delivered to Customer as part of the Subscription Services, Consulting Services or Support Services then Customer shall receive a limited license consistent with the terms of Section 2 to use such materials during the Subscription Period.

2.6 Customer's Responsibilities. Customer will: (i) be responsible for meeting Accela's applicable minimum system requirements for use of the Subscription Services set forth in the Documentation; (ii) be responsible for Authorized Users' compliance with this Agreement and for any other activity (whether or not authorized by Customer) occurring under Customer's account; (iii) be solely responsible for the accuracy, quality, integrity and legality of Customer Data; (iv) use commercially reasonable efforts to prevent unauthorized access to or use of the Subscription Services and Customer Data under its account, and notify Accela promptly of any such unauthorized access or use, and; (v) use the Subscription Services only in accordance with the applicable Documentation, laws and government regulations.

3. PAYMENT TERMS.

3.1 Purchases Directly from Accela. Except as otherwise set forth in an Order, Subscription fees shall be invoiced annually in advance and such fees shall be due and payable on the first day of the Subscription and on each anniversary thereafter for each renewal, if any. All other invoices shall be due and payable net thirty (30) from the date of the applicable invoice. All amounts payable to Accela under this Agreement shall be paid by Customer in full without any setoff, deduction, debit, or withholding for any reason. Any late payments shall be subject to an additional charge of the lesser of 1.5% per month or the maximum permitted by law. All Subscription Services fees are exclusive of any taxes, levies, duties, withholding or similar governmental assessments of any nature (collectively, "**Taxes**"). If any such Taxes are owed or payable for such transactions, they shall be paid separately by Customer without set-off to the fees due Accela.

3.2 Reserved.

4. CONFIDENTIALITY. As used herein, "**Confidential Information**" means all confidential information disclosed by a one party to this Agreement to the other party of this Agreement whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. However, Confidential Information will not include any information that: (i) is or becomes generally known to the public without breach of any obligation owed to the disclosing party; (ii) was known to the receiving party prior to its disclosure without breach of any obligation owed to the disclosing party; (iii) is received without restriction from a third party without breach of any obligation owed to the disclosing party; or (iv) was independently developed by the receiving party. Each party will use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) not to disclose or use any Confidential Information except as permitted herein, and will limit access to Confidential Information to those of its employees, contractors and agents who need



such access for purposes consistent with this Agreement and who are bound to protect such Confidential Information consistent with this Agreement. The receiving party may disclose Confidential Information if it is compelled by law to do so, provided the receiving party gives the disclosing party prior notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the disclosing party's request and cost, to contest, limit, or protect the disclosure.

5. CUSTOMER DATA.

5.1 Ownership. Customer reserves all its rights, title, and interest in and to the Customer Data. No rights are granted to Accela hereunder with respect to the Customer Data, except as otherwise set forth explicitly in Section 5.

5.2 Usage. Customer shall be responsible for Customer Data as entered in to, applied or used in the Subscription Services. Customer acknowledges that Accela generally does not have access to and cannot retrieve lost Customer Data. Customer grants to Accela the non-exclusive right to process Customer Data (including personal data) for the sole purpose of and only to the extent necessary for Accela: (i) to provide the Subscription Services; (ii) to verify Customer's compliance with the restrictions set forth in Section 2.4 (Restrictions on Use) if Accela has a reasonable belief of Customer's non-compliance; and (iii) as otherwise set forth in this Agreement. Accela may utilize the information concerning Customer's use of the Subscription Services (excluding any use of Customer's Confidential Information) to improve Subscription Services, to provide Customer with reports on its use of the Subscription Services, and to compile aggregate statistics and usage patterns by customers using the Subscription Services.

5.3 Use of Aggregate Data. Customer agrees that Accela may collect, use and disclose Aggregate Data derived from the use of the Subscription Services for industry analysis, benchmarking, analytics, marketing and other business purposes. All Aggregate Data collected, used and disclosed will be in aggregate form only and will not identify Customer, its Authorized Users or any third parties utilizing the Subscription Services.

6. WARRANTIES AND DISCLAIMERS.

6.1 Subscription Services Warranty. During the Subscription Period, Accela warrants that Subscription Services shall perform materially in accordance with the applicable Documentation. As Customer's sole and exclusive remedy and Accela's entire liability for any breach of the foregoing warranty, Accela will use commercially reasonable efforts to: (a) repair the Subscription Services in question; (b) replace the Subscription Services in question with those of substantially similar functionality; or (c), after making all commercially reasonable attempts to do the foregoing, terminate the applicable Subscription Services and refund all unused, prepaid fees paid by Customer for such non-compliant Subscription Services.

6.2 Consulting Services Warranty. For ninety (90) days from the applicable delivery, Accela warrants that Consulting Services shall be performed in a professional and workmanlike manner. As Customer's sole and exclusive remedy and Accela's entire liability for any breach of the foregoing warranty, Accela will use commercially reasonable efforts to (a) re-perform the Consulting Services in a compliant manner; or, after making all commercially reasonable attempts to do the foregoing, (b) refund the fees paid for the non-compliant Consulting Services.

6.3. Disclaimers. EXCEPT AS EXPRESSLY PROVIDED HEREIN, ACCELA MAKES NO WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, SECURITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.



6.4. Cannabis-Related Activities. If Customer purchases any Subscription Services for use with any cannabis-related activities, the following additional disclaimers shall apply: Accela is considered a software service provider to its customers and not a cannabis related business or agent thereof. In addition to the foregoing, Accela only retains Subscription Services fees of this Agreement from its Customer for general software services, a state or local government agency, and does not retain these fees from any type of External Users. It is the sole responsibility of the Customer to offer state law compliant services, which may be coordinated and facilitated through the use of the Subscription Services. Accela makes no representations, promises, or warranties with respect to the legality, suitability, or otherwise regarding any third party provider, including partners, and have no responsibility or liability with respect to services provided to Customer by such third parties.

7. **INDEMNIFICATION.** Accela will defend (or at Accela's option, settle) any third party claim, suit or action brought against Customer to the extent that it is based upon a claim that the Subscription Services, as furnished by Accela hereunder, infringes or misappropriates the Intellectual Property Rights of any third party, and will pay any costs, damages and reasonable attorneys' fees attributable to such claim that are finally awarded against Customer, provided that Customer provides: (a) Accela notice of such claim as soon practical and in no event later than would reasonably permit Accela to respond to such claim, (b) reasonable cooperation to Accela, at Accela's expense, in the defense and/or settlement of such claim and (c) Accela the sole and exclusive control of the defense, litigation and settlement of such claim. In the event that Accela reasonably believes, in its sole discretion, that such claim may prevail or that the usage of the Subscription Services may be joined, Accela may seek to: (a) modify the Subscription Services such that it will be non-infringing (provided such modification does not materially reduce the functionality or performance of Customer's installed instance); (b) replace the Subscription Services with a service that is non-infringing and provides substantially similar functionality and performance; or, if the first two options are not commercially practicable, (c) terminate the remainder of the Subscription Period and refund any, pre-paid, unused fees received by Accela. Accela will have no liability under this Section 7 to the extent any claims arise from (i) any combination of the Subscription Services with products, services, methods of a third party; (ii) a modification of the Subscription Services that were either implemented by anyone other than Accela or implemented by Accela in accordance with Customer specifications; (iii) any use of the Subscription Services in a manner that violates this Agreement or the instructions given to Customer by Accela; (iv) a version of the Subscription Services other than the current, fully patched version, provided such updated version would have avoided the infringement; or (v) Customer's breach of this Agreement. THIS SECTION 7 STATES THE ENTIRE OBLIGATION OF ACCELA AND ITS LICENSORS WITH RESPECT TO ANY ALLEGED OR ACTUAL INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS RELATED TO THIS AGREEMENT.

8. **LIMITATION OF LIABILITY.** EXCEPT FOR LIABILITY ARISING OUT OF EITHER PARTY'S LIABILITY FOR DEATH OR PERSONAL INJURY OR CUSTOMER'S BREACH OF SECTION 2, NEITHER PARTY'S AGGREGATE LIABILITY FOR DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR FROM THE USE OF OR INABILITY TO USE THE SERVICE, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, SHALL EXCEED TWO (2) TIMES THE TOTAL AMOUNT PAID BY CUSTOMER HEREUNDER IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE INCIDENT. EXCEPT FOR LIABILITY ARISING OUT OF CUSTOMER'S BREACH OF SECTION 2 OR EITHER PARTY'S LIABILITY FOR DEATH OR PERSONAL INJURY, IN NO EVENT SHALL EITHER PARTY OR ANY OTHER PERSON OR ENTITY INVOLVED IN CREATING, PRODUCING OR DELIVERING THE SERVICE BE LIABLE FOR ANY INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, INCLUDING LOST PROFITS, LOSS OF DATA OR LOSS OF GOODWILL, SERVICE INTERRUPTION, COMPUTER DAMAGE OR SYSTEM



FAILURE OR THE COST OF SUBSTITUTE PRODUCTS OR SERVICES, ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT OR FROM THE USE OF OR INABILITY TO USE THE SUBSCRIPTION SERVICES, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR ANY OTHER LEGAL THEORY. THE FOREGOING EXCLUSIONS APPLY WHETHER OR NOT A PARTY HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGE, AND EVEN IF A LIMITED REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

9. **SECURITY.** Accela has implemented commercially viable and reasonable information security processes, policies and technology safeguards to protect the confidentiality and integrity of Customer Data, personal data protect against reasonably anticipated threats. Customer acknowledges that, notwithstanding security features of the Subscription Services, no product, hardware, software or service can provide a completely secure mechanism of electronic transmission or communication and that there are persons and entities, including enterprises, governments and quasi- governmental actors, as well as technologies, that may attempt to breach any electronic security measure. Subject only to its limited warranty obligations set forth in Section 6, Accela will have no liability for any such security breach. Customer further acknowledges that the Subscription Services is not guaranteed to operate without interruptions, failures, or errors. If Customer or Authorized Users use the Subscription Services in any application or environment where failure could cause personal injury, loss of life, or other substantial harm, Customer assumes any associated risks and will indemnify Accela and hold it harmless against those risks.

10. **THIRD PARTY SERVICES.** Customer may choose to obtain a product or service from a third party that is not directly produced by Accela as a component of the Subscription Services ("***Third Party Services***") and this may include third party products resold by Accela. Accela assumes no responsibility for, and specifically disclaims any liability, warranty or obligation with respect to, any Third Party Service or the performance of the Subscription Services (including Accela's service level commitment) when the Subscription Services are used in combination with or integrated with Third Party Services.

11. **TERM AND TERMINATION.**

11.1 **Agreement Term.** This Agreement shall become effective on the Effective Date and shall continue in full force and effect until the expiration of any Subscription Periods set forth in an applicable Order governed by the Agreement.

11.2 **Subscription Periods & Renewals.** Subscription Periods begin as specified in the applicable Order and, unless terminated earlier in accordance with this Agreement, continue for the term specified therein. Subscription Services renewals may be subject to an annual increase, for which Accela shall provide Customer notice prior to the renewal of the Subscription Period. In the event of any non-renewal or other termination, Customer's right to use the Subscription Services will terminate at the end of the relevant Subscription Period.

11.3 **Termination or Suspension for Cause.** A party may terminate this Agreement and Subscription Services license granted hereunder for cause upon thirty (30) days' written notice to the other party of a material breach if such breach remains uncured at the expiration of such thirty (30) day period. Either party may terminate immediately if the other party files for bankruptcy or becomes insolvent. Accela may, at its sole option, suspend Customer's or any Authorized User's access to the Subscription Services, or any portion thereof, immediately if Accela: (i) suspects that any person other than Customer or an Authorized User is using or attempting to use Customer Data; (ii) suspects that Customer or an Authorized User is using the Subscription Services in a way that violates this Agreement and could expose Accela or any other entity to harm or legal liability; (iii) is or reasonably believes it is required to



do so by law or court order or; (iv) Customer's payment obligations are more than ninety (90) days past due, provided that Accela has provided at least thirty (30) days' notice of such suspension for delinquent payment. Should Customer terminate this Agreement for cause, Accela will refund a pro-rata portion of unused, pre-paid fees.

11.4 Effect of Termination. If this Agreement expires or is terminated for any reason: (i) within thirty (30) calendar days following the end of Customer's final Subscription Period, upon Customer's request Accela provided Customer Data and associated documents in a database dump file; provided that Customer pays (a) all costs of and associated with such copying, as calculated at Accela's then-current time-and-materials rates, and (b) any and all unpaid amounts due to Accela; (ii) licenses and use rights granted to Customer with respect to Subscription Services and intellectual property will immediately terminate; and (iii) Accela's obligation to provide any further services to Customer under this Agreement will immediately terminate, except as mutually agreed between the parties. If the Subscription Services are nearing expiration date or are otherwise terminated, Accela will initiate its data retention processes, including the deletion of Customer Data from systems directly controlled by Accela. Accela's current Data Storage Policy can be accessed www.accela.com/terms/.

11.5 Survival. Sections 2.5 (Ownership and Proprietary Rights), 4 (Confidentiality), 6.3 (Disclaimer), 8 (Limitation of Liability), 11.4 (Effect of Termination), 11.5 (Surviving Provisions), and 12 (General Provisions) will survive any termination or expiration of this Agreement.

12. GENERAL.

12.1 Notice. Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder will be in writing and will be deemed to have been given upon: (i) personal delivery; (ii) three days after sending registered, return receipt requested, post or; (iii) one day after sending by commercial overnight carrier. Notices will be sent to the address specified by the recipient in writing when entering into this Agreement or establishing Customer's account for the Subscription Services.

12.2 Reserved.

12.3 Compliance with Laws. Each party will comply with all applicable laws and regulations with respect to its activities under this Agreement including, but not limited to, export laws and regulations of the United States and other applicable jurisdictions. Further, in connection with the services performed under this Agreement and Customer's use of the Subscription Services, the parties agree to comply with all applicable anti-corruption and anti-bribery laws, statutes and regulations.

12.4 Assignment. Customer may not assign or transfer this Agreement, whether by operation of law or otherwise, without the prior written consent of Accela, which shall not be unreasonably withheld. Any attempted assignment or transfer, without such consent, will be null and void. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.

12.5 Publicity. Notwithstanding anything to the contrary, each party will have the right to publicly announce the existence of the business relationship between parties without disclosing the specific terms of the Agreement.

12.6 Miscellaneous. No failure or delay by either party in exercising any right under this Agreement will constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a party at law or in equity. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be modified by the court and interpreted so as best to accomplish the objectives of the original provision to



the fullest extent permitted by law, and the remaining provisions of this Agreement will remain in effect. Accela will not be liable for any delay or failure to perform under this Agreement to the extent such delay or failure results from circumstances or causes beyond the reasonable control of Accela. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or similar relationship between the parties. This Agreement, including any attachments hereto as mutually agreed upon by the parties, constitute the entire agreement between the parties concerning its subject matter and it supersedes all prior communications, agreements, proposals or representations, written or oral, concerning its subject matter. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in writing and signed by a duly authorized representative of each party against whom the modification, amendment or waiver is to be asserted. Notwithstanding any language to the contrary, no additional or conflicting terms or conditions stated in any of Customer's purchase order documentation or otherwise will be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.



Statement of Work
Patient Registry/Verification and
Cannabis Businesses Licensing

South Dakota
Department of Health
Department of Revenue

September 9, 2021

Table of Contents

REVISION LOG.....	3
DELIVERABLES AND PRICING	4
PAYMENT SCHEDULE.....	6
CHANGE CONTROL	6
DELIVERABLE ACCEPTANCE	8
PRELIMINARY PROJECT SCHEDULE.....	9
CANNABIS BUSINESS PROCESSES.....	10
DETAILED STATEMENT OF WORK DESCRIPTION	12
DELIVERABLE 1: PROJECT INITIATION.....	12
DELIVERABLE 2: CIVIC PLATFORM SETUP	13
DELIVERABLE 3: RECORD TYPE GAP ANALYSIS SESSIONS	14
DELIVERABLE 4: RECORD TYPE CONFIGURATION.....	14
DELIVERABLE 5: XAPO (ADDRESS, OWNER, PARCEL INFORMATION)	16
DELIVERABLE 6: BUSINESS PROCESS VALIDATION	16
DELIVERABLE 7: INTERFACE ANALYSIS AND DEVELOPMENT.....	17
DELIVERABLE 8: ACCELA CITIZEN ACCESS CONFIGURATION.....	19
DELIVERABLE 9: ACCELA APPS CONFIGURATION	20
DELIVERABLE 10: REPORT CONFIGURATION.....	20
DELIVERABLE 11: TRAINING.....	21
DELIVERABLE 12: USER ACCEPTANCE TESTING (UAT).....	22
DELIVERABLE 13: POST DEPLOYMENT SUPPORT.....	23
CONTINGENCY IMPLEMENTATION.....	24
PROJECT MANAGEMENT	24

REVISION LOG

This log provides a synopsis of revisions made to this document.

Version	Date	Author	Description
1.0	09/08/2021	Brian Heath	Initial Document
1.1	09/09/2021	Anne Szkatulski	Added Introduction

INTRODUCTION

This Statement of Work ("SOW") dated September 9, 2021 sets forth the scope and definition of the project-based professional services (collectively, the "Services") to be provided by Accela, Inc., its affiliates and/or agents ("Accela") to the State of South Dakota Departments of Health and Revenue (together "State" or "Agency").

EXECUTIVE SUMMARY

This document outlines the configuration and onboarding activities that are included with the State's Accela Cannabis Solution, captures our understanding of what configurations the State will receive, and provides visibility into how Accela will perform the onboarding of your solution.

SOLUTION OVERVIEW

Your subscription includes the following SaaS products, as defined in the applicable Order Form:

- Accela Civic Applications
 - Cannabis Licensing
- cloudPWR Patient Registry/Verification

DELIVERABLES AND PRICING

DELIVERABLES AND PRICING	
DELIVERABLE 1: PROJECT INITIATION	\$5,000.00
DELIVERABLE 2: SETUP – DEV, TEST and PRODUCTION	\$2,500.00
DELIVERABLE 3: RECORD TYPE ANALYSIS SESSIONS	\$3,125.00
DELIVERABLE 4: RECORD TYPE CONFIGURATION	\$4,375.00
DELIVERABLE 5: ACCELA XAPO - ADDRESS PARCEL OWNER	\$7,500.00
DELIVERABLE 6: BUSINESS PROCESS VALIDATION AND AUTOMATION	\$16,250.00
DELIVERABLE 7: INTERFACE ANALYSIS AND DEVELOPMENT	\$10,000.00
DELIVERABLE 7A: ACCELA ESRI INTEGRATION	\$3,000.00
DELIVERABLE 7B: PAYMENT GATEWAY INTEGRATION	\$3,000.00
DELIVERABLE 7C: ACCELA SEED TO SALE INTEGRATION	\$15,000.00
DELIVERABLE 8: CITIZEN ACCESS WEB PORTAL CONFIGURATION	\$16,250.00
DELIVERABLE 9: ACCELA APPS CONFIGURATION	\$2,000.00
DELIVERABLE 10: REPORTS	\$17,500.00
DELIVERABLE 11: TRAINING	\$13,500.00
DELIVERABLE 12: USER ACCEPTANCE TESTING (UAT)	\$12,500.00
DELIVERABLE 13: POST DEPLOYMENT SUPPORT	\$10,000.00
CONTINGENCY IMPLEMENTATION FOR ACCELA	\$15,000.00
PROJECT MANAGEMENT	\$14,625.00
TOTAL	\$176,125.00

The above table is an estimate of costs associated with individual deliverables. The project will be delivered on an hourly payment basis.

*For the Business Licensing solution, a billing rate of \$125/hour for services will be used throughout the project.

*For the Patient Registry/Verification System, a fixed fee for services up to 160 hours at a billing rate of \$250/hour has been applied for this project.

PAYMENT SCHEDULE

Accela will perform the Services on an hourly payment basis based on: (i) the nature and scope of the Services (ii) the expected staffing requirements, (iii) the Project Schedule, (iv) Accela's and Agency's roles and responsibilities, and (v) the other assumptions as set forth in this SOW. The projects is expected to take 1,249 hours, with 1,089 hours at a rate of \$125 per hour (the "**Hourly Rate**" for for the Business Licensing solution) and 160 hours at a rate of \$250 per hour (the "**Hourly Rate**" for the Patient Registry/Verification System); **Accela's total price to perform the Services is estimated to be \$176,125.00**, exclusive of taxes and expenses. This estimated price is based on the information available at the time of signing and the assumptions, dependencies and constraints, and roles and responsibilities of the Parties, as stated in this SOW. Accela will not (i) exceed the total estimate amount without the prior approval of Agency and/or (ii) continue to provide Services, after the total estimate has been reached, without the prior authorization of Agency. Should there be changes to the scope, timeline or resources that increases the hours or costs needed to complete the Project, a Change Order may be required prior to project continuation. Please see Change Control section.

Any estimated hours remaining on the Project when Accela has completed the scope or this project will not be used for other work without a Change Order delineating the scope. Any estimated hours remaining on the project when Accela has completed work will either terminate when the scope has been completed or expire on the term date of the Agreement, whichever is sooner.

Invoices will be sent for hours worked monthly. Payments are due net 30 of the invoice date.

EXPENSES

There is no provision for travel expenses or travel time in this SOW because Agency does not need any onsite resources. Travel to the Agency will not be conducted unless a Change Order, inclusive of travel expense terms and conditions, is signed prior to travel commencing to cover the cost of the travel.

CHANGE CONTROL

We will utilize change control management. This process estimates the impact on the project if the client requests changes to the scope of the project or if additional hours are needed to complete an estimated task. This procedure also helps us to advise clients of adjustments to the schedule and/or the total cost for any change and authorizes us to proceed on approved changes.

Our change control documents will itemize all of the requested changes, noting the item's priority and cost and schedule impact. Using this document, the Agency may determine what changes are truly necessary in order to meet their business needs and stay within the acceptable budget and schedule.

When the scope of the change has been finalized, we will issue a Change Order Authorization document, listing the final change items, budget, and schedule impact. When the Change Order Authorization has been approved and signed, we will add the additional tasks or hours to the schedule.

EXPIRATION

The scope and terms of this SOW must be executed within sixty (60) calendar days of the date of this SOW. If the SOW is not executed within that timeframe, the current scope and terms can be renegotiated.

DISCLAIMERS

Accela makes no warranties in respect of its Services described in this SOW except as set out in the Agreement. Any configuration of or modification to the Product that can be consistently supported by Accela via APIs, does not require direct database changes and is capable of being tested and maintained by Accela will be considered a "Supported Modification". Accela's obligations and warranties in respect of its Services, Products, and maintenance and support, as set out the agreement between Accela and Agency, does not extend outside the Supported Modifications or to any Agency manipulation of implemented scripts, reports, integrations and adaptors.

DELIVERABLE ACCEPTANCE

A

B

Tel: _____

Date: _____

Agency Name: _____

Approving Agency Manager: _____

Byrne/cloudPWR Manager: _____

Project Name / Code: _____

Contract / Agreement #: _____

Agency agrees that Accela has successfully completed the following Deliverables:

Deliverable #	Source /
	Reference
	Details
	Service
	Agreement

Agency agrees that Accela has successfully completed the Deliverables described above in accordance with the terms of the related Contract/Agreement.

APPROVALS:

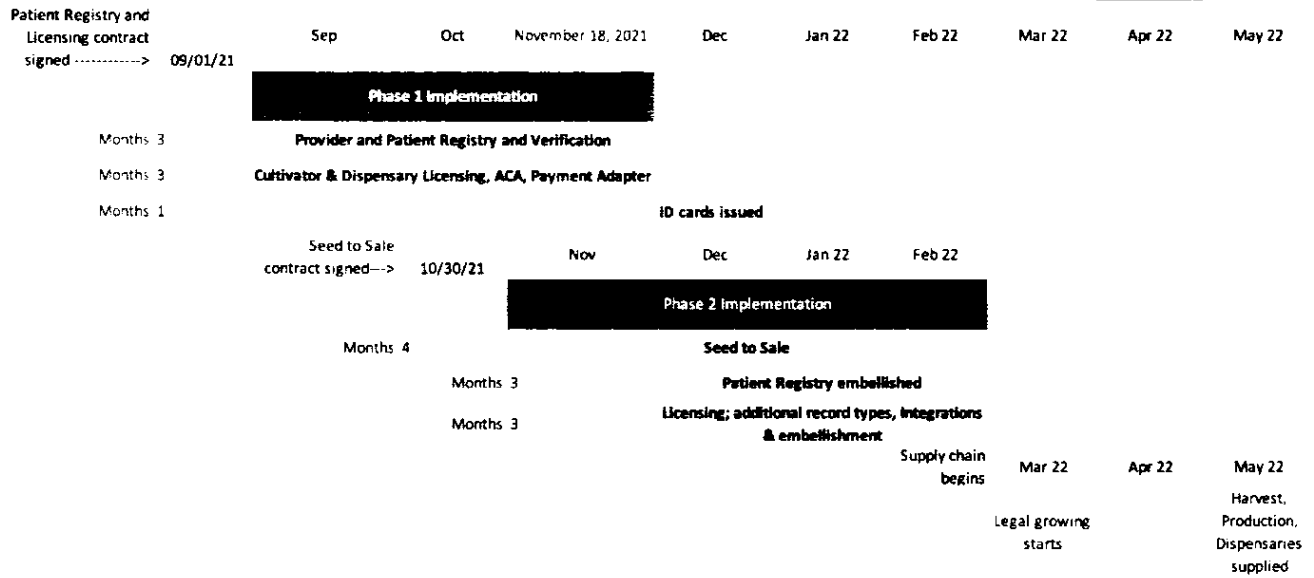
Agency Name

Signature

Title

Date

PRELIMINARY PROJECT SCHEDULE





CANNABIS BUSINESS PROCESSES

Cards/Licenses

- Patient Registry & Medical ID Cards/Verification
- Medical Cannabis Business Licensing

Integrations

- AGIS (Accela-Esri Connector)
- Payment Processor (Assumes Accela Standard Payment Adapter: forte, PayPal, Official Payments Co-Brand, Official Payments STP, or Elavon)
- Seed-to-Sale

Proposed

- Accela Cannabis Regulation
- cloudPWR Patient Registry

Knowledge Transfer:

We will make all reasonable efforts to transfer knowledge to the State. It is critical that State personnel participate in the analysis, configuration and deployment of the Patient Registry/Verification and Businesses Licensing as part of this transfer, so that after go-live assistance tasks are completed, the State will be self-sufficient in its operation and use.

We leverage an Agile implementation methodology to identify and prioritize the requirements and allow for an iterative, high quality, go-live process. This is proven methodology that provides the State the most optimized way to implement a quality project on time and on budget.

The Accela Project Management will successfully guide the State through the Agile approach.

We focus on building and delivering in smaller increments, called iterations.

- They create a list with our customers, known as a “project to-do list” or “product backlog” that defines each of the individual features and requirements.
- Using Agile estimation techniques, they roughly estimate the effort for each task.
- We then work with the State to prioritize the task list.
- Next, we propose a number of tasks to complete over the coming 1-2-week period; sprint.
- At the end of the sprint, we conduct a show and tell with the State, in order to show what’s been done and how many points were completed, to gather feedback and discuss any issues and to plan out the next 2 weeks of tasks.
- At the end of the sprint, they also conduct an internal meeting, known as a “retrospective”, where each member of the team reviews what went well, what didn’t work well and what can be done to improve the process going forward.

We provide each client with solution documentation. This documentation is provided at no additional charge since it is inherently part of the implementation tools and documents that are necessary to give users and system administrators’ knowledge about the facets and operation of the system.

Accela provides the State with the one soft copy in portable document file (.pdf) format, of all documentation necessary for the Accela solutions acquired under future programs. The State will have

the right of reproduction so that as many copies can be made of the documentation as necessary for training or subsequent purposes.

Additionally, Accela will provide State with user training manual document templates in Microsoft Word format, which can be customized with screenshots specific to the State's system. System Administrators and other IT professionals are provided comprehensive standard administrator manuals for the platform purchased. Additionally, support documentation, notes and other reference materials are provided on Accela Customer Success Community.

The project SharePoint will serve as a repository for all of the documentation developed during the implementation; i.e. statement of work, project charter, project plan, communication plan, requirements, design specifications, test documents, end-user guides.

Interoperability:

In order to determine the State's requirements for interfaces, analysis sessions will be conducted with the State. The findings will then be documented in the Interface Specifications Document(s) for our use in building the interface code. The implementation of the interface is dependent on the assistance of the State's staff, specifically, interface analysis, data mapping, and data manipulation as required in the source system. We will provide a solution utilizing APIs to interface with third party systems.

DETAILED STATEMENT OF WORK DESCRIPTION

The following section describes the specific activities and tasks that will be executed to meet the business objectives and business requirements of the Agency. In support of the implementation effort as described above, Accela will provide the following detailed implementation services. For each deliverable, a description is provided as well as criteria for acceptance of the deliverable.

DELIVERABLE 1: PROJECT INITIATION

Project initiation is an opportunity to ensure the project starts in a well-organized, structured fashion while re-confirming the Agency and Accela's expectations regarding the implementation. This Deliverable is comprised of project planning activities, core project management documents and templates and the first meeting conducted between the Agency and Accela.

In conjunction with the Agency representatives, Accela will perform the following tasks:

- Finalize staffing for the project teams.
- Conduct a formal Kickoff meeting. The objective of this meeting is to review the purpose of the project and discuss the project scope, roles and responsibilities, deliverables, and timeline.
- Provide Accela standard Project Status Report Template format.
- Finalize and document formal deliverable signoff procedures, identify team members that will be responsible for signoff from the Agency.
- Finalize an integrated baseline project plan that includes resource allocation for all tasks (in cooperation with the Agency Project Manager).

The Project Kickoff Meeting includes a formal presentation by the project team to review project objectives, methodology, timeline, roles and responsibilities, risks, and other key project elements with project stakeholders.

In terms of specific output, the following will be executed for this deliverable:

- Baseline Project Plan
- Project Status Report Template
- Project Kickoff Presentation

Our Responsibilities:

- Provide timely and appropriate responses to Agency's request for information.
- Coordinate project planning activities.
- Communicate the Implementation Methodology that will be used by Accela to deliver Services.
- Complete Baseline Project Plan, Project Status Report Template, and Project Kickoff Presentation deliverables with input from appropriate Agency resources.

Agency Responsibilities:

- Identify and set expectations with key resources and subject matter experts for ongoing participation in the project.
- Provide timely and appropriate responses to Accela's requests for project planning input and meeting logistics requests.
- Provide meeting facilities for Project Kickoff and other onsite activities.
- Include Project Sponsor in Project Kickoff Meeting.
- Provide suitable Agency facilities to accommodate training.
- Ensure that users are proficient in using PC's in a Windows environment as a prerequisite for the training.
- Ensure that users are familiar with use of standard Internet browsers as a prerequisite for the training.

Acceptance Criteria:

- Review and acceptance of the Project Status Report Template
- Review and acceptance of the Baseline Project Plan
- Completion of the Project Kickoff Meeting

DELIVERABLE 2: CIVIC PLATFORM SETUP

Upon Contract signing, Accela will setup an environment in the Cloud and load the package solutions for the Cannabis App/cloudPWR and all related elements.

In terms of specific output, the following will be executed for this deliverable:

- Verify that the Accela Civic Platform and cloudPWR Patient Registry / Verification infrastructure are operational by using the valid credentials to log into the Agency's computing environment.

Our Responsibilities:

- Provide timely and appropriate responses to Agency's request for information.
- Setup the Accela Civic Platform and Patient Registry / Verification infrastructure in the Cloud.
- Provide desktop requirements documentation to Agency.
- Provide instructions on how to login/logout and view the loaded Standard Package Solutions

Agency Responsibilities:

- Provide timely and appropriate responses to requests for information by Accela.
- Arrange for the availability of appropriate Agency staff to assist with inquires and activities related to system installation, setup, testing, and quality assurance throughout the setup process.
- Schedule appropriate Agency staff participants and meeting locations for activities.

Acceptance Criteria:

- Confirmation of ability to log into the Civic Platform and Patient Registry / Verification using the valid credentials

DELIVERABLE 3: RECORD TYPE GAP ANALYSIS SESSIONS

We will work closely with designated Agency personnel and will conduct analysis sessions to capture and align Accela Civic Apps with Agency business processes. A part of the process mapping is to group “like” processes together to assist in streamlining the analysis and minimize redundancy.

In terms of specific output, the following will be executed for this deliverable:

- Best Practice Business Process Gap Analysis document.
- Accela has allotted up to 25 hours to this effort for Business Licensing
- Accela is fixed-fee up to 25 hour for Patient Registry / Verification
- Additional efforts required outside this scope can be addressed via the Change Order process

Our Responsibilities:

- Provide timely and appropriate responses to the Agency’s request for information.
- Conduct meetings via email, web conference, phone, and in person to gather and validate analysis.
- Create Gap Analysis documents for each record type for Agency approval.

Agency Responsibilities:

- Provide timely and appropriate responses to Accela’s requests for information.
- Make available the appropriate Agency key staff.
- Provide any existing fee schedules and other pertinent document samples.
- Schedule participants and meeting locations for analysis activities.

Acceptance Criteria:

- Completion of To Be Gap Analysis documents for Best Practice Record Types to be configured.

DELIVERABLE 4: RECORD TYPE CONFIGURATION

Accela resources will update the Accela Civic Apps based on the gap analysis documents produced during analysis sessions and approved by the Agency. This includes the addition of custom fields to support any unique business processes by the agency, any fields required to maintain information from legacy systems, or any configuration updates in the workflows or fees that are unique to the agency.

The following list provides examples of the types of updates that may be required per use case;

- Add or rename existing fields in order to account for Agency business processes and/or data conversion mapping.
- Define and create user accounts with associated user groups/security access.
- Updates to existing workflows as needed
- Updates to existing system dropdown fields
- Updates and creation of Agency specific fee schedules
- Updates and creation of Agency specific inspection types and guide sheets/checklists
- Others areas as defined

In terms of specific output, the following will be executed for this deliverable:

- Accela has allotted up to 35 Hours to Business Licensing configuration
- Accela is fixed-fee up to 20 Hours for Patient Registry / Verification
- Additional efforts required outside this scope can be addressed via the Change Order process
- Documentation of each configuration per use case

Our Responsibilities:

- Provide timely and appropriate responses to Agency's request for information.
- Interview staff in order to understand existing business processes.
- Conduct requested sessions to capture the required business processes to be automated within the system.
- Conduct meetings via email, web conference, phone, and in person to complete required consulting.

Agency Responsibilities:

- Provide timely and appropriate responses to Accela's requests for information.
- Make available the appropriate Agency key users and content experts to provide required information, participate in the configuration analysis and verify the accuracy of the documented workflows, input/output formats, and data elements.
- Provide any existing business process documentation, including process flows; fee schedules; commonly used applications, reports and forms; and other relevant information
- Schedule participants and meeting locations for analysis activities.

Acceptance Criteria:

- Types in accordance with the approved To Be Gap Analysis Documents in the Agency Cloud Environment.

DELIVERABLE 5: XAPO (ADDRESS, OWNER, PARCEL INFORMATION)

Accela resources will work with the agency in gathering all of the necessary information from GIS and perform the configuration tasks required for the built in integration. Agency can utilize all available parcel, address and owner attribute fields to populate with GIS data.

Our Responsibilities:

- Work with agency staff to identify links, layers and services to connect to Accela
- Provide guidance to agency staff on what is required in GIS for the integration to work
- Perform all configuration activities to pull address, parcel and owner data using the built in interface.

Agency Responsibilities:

- Provide timely and appropriate responses to Accela's requests for information.
- Provide information on the GIS environment and ensure that it meets the minimum standards required for the Accela integration

Acceptance Criteria:

- Demonstrate retrieval of GIS address, parcel and owner data in the Accela Civic Platform environments

DELIVERABLE 6: BUSINESS PROCESS VALIDATION

During the configuration analysis phase of the implementation project, Accela will identify opportunities to supplement the Accela Civic Platform base functionality via Accela Event Manager Script Engine (EMSE) scripts and Expression Builder in order to validate and automate business processes. Accela will work with Agency to identify desired functionality, and subsequently will assist with prioritizing the needs in order to determine that will be developed by Accela within the scope of this implementation. The Business Process Validation and Civic Platform developed by Accela can be used as models whereby agency staff can develop and modify additional functionality as needed.

- **EMSE (Event Manager Scripting Engine)** – used to script based on system activities, such as a before or after event, that allow the system to automate activities (**example:** do not allow an inspection to be scheduled prior to a specific workflow task, or, auto-calculate and invoice a fee upon application submittal)
- **Expression Builder** – used to script form based interactions that occur prior to triggering and event or master script activity (**example:** auto-population form based data fields based on user-selected values)

During the configuration analysis phase of the implementation project, Accela will identify opportunities to supplement the Patient Registry Verification System. Business Process Validation is supported by the following.

- **Verification Workflow Engine** - used to execute business logic based upon a wide variety of triggers.

Prior to the development, the Agency will approve a design specification document that will be created jointly by the Agency and Accela. The approved document will be used as a basis for determining completion and approval of the deliverable.

In terms of specific output, the following will be executed for this deliverable:

- Prioritized list of requirements for Patient Registry/Verification and Business Licensing Solution
- **Specification documents for the Patient Registry/Verification and Business Licensing Solution**
- **Demonstration of completed Patient Registry/Verification and Business Licensing Solution in development or test environments per the specifications document(s)**
- Accela has allotted up to 50 hours for Business Licensing
- Accela is fixed-fee up to 25 hours for Patient Registry / Verification

Our Responsibilities:

- Work with Agency staff to identify potential uses of scripting
- Assist with development of list of desired functionality
- Aid the Agency in prioritizing which scripts will be developed by Accela
- Develop scripts based on the specifications
- Demonstrate functionality of scripts per specifications

Agency Responsibilities:

- Allocate the time for qualified business and technical experts for the script requirements sessions that are critical to the project success
- Identify resources that will learn scripting tools and approaches for ongoing maintenance
- Prioritize desired functionality to determine which scripts Accela will develop
- Provide timely and appropriate responses to Accela's request for information
- Verify the Script Specification meets the intended business requirement
- Allocate the time for qualified personnel to test the script for acceptance

Acceptance Criteria:

- Review and acceptance of design document with written sign-off from the Agency
- Demonstration of all developed script within the system to the Agency

DELIVERABLE 7: INTERFACE ANALYSIS AND DEVELOPMENT

- ESRI Integration

- Accela will provide a program to integrate 3rd Party data to/from Accela Civic Platform.
 - Not applicable to Patient Registry
- Payment Gateway Integration
 - Accela will provide a program to integrate 3rd Party data to/from Accela Civic Platform. For Business Licensing, the Payment Adapter assumes one of the current Accela Business Licensing out-of-the box payment adapters only: PayPal, Official Payments CoBrand, forte, or Virtual Merchants/Elavon
 - For the Patient Registry/Patient Verification System we will provide an API to interface to a payment processor system
- Seed-to-Sale Integration
 - The State is in the process of selecting and contracting for a Seed To Sale system. Installation of the Seed to Sale system would logically fall into Phase 2 of the Preliminary Project Schedule presented on page 7 of this Statement of Work.
 - To determine the Agency requirements for this interface, analysis sessions will be conducted as a portion of this deliverable. Accela will collaborate with the State and its contractor for the Seed to Sale System to document the Interface Specifications to be used by Accela in building the interface code.
 - The implementation of the interface is dependent on the assistance of the Agency's staff, specifically, interface analysis, data mapping, and data manipulation as required in the source system.

In terms of specific output, the following will be executed for this deliverable:

- Interface Specifications Document
- Operational Interface in the Development, Test and Production environments

Our Responsibilities:

- Provide timely and appropriate responses to Agency's request for information.
- Conduct Interface Analysis sessions.
- Work with Agency staff to develop interface specifications document.
- Use an Accela web service or other tool to implement the interface functionality based on the specifications.
- Build all aspects of the interface that interact directly with the Accela Civic Platform.

Agency Responsibilities:

- Provide timely and appropriate responses to Accela's request for information.
- Provide system and access to individuals to provide required details of system interface.
- Allocate the time for qualified business and technical experts for the testing sessions that are critical to the project success.
- Identify and coordinate any related tools used to implement the interface (3rd party or in-house development).
- Assist in the interface specification development and data mapping process.
- Review and approve the interface specification documents.
- Work with Third Party Data Sources to determine best methods of interfacing to Accela system.
- Validate interface through testing.

- Work with 3rd party to ensure data from Accela is in correct format.
- Updates to interface, post go-live, due to changes in 3rd party system or Agency business processes.

Acceptance Criteria:

- Review and approve the Interface Specifications document.
- Demonstration and approval of the completed interface as per the requirements detailed in the interface specifications document in the Test, Dev & Production environments.

Acceptance Review Period:

- Two (2) business days total (due to Legislative deadline)

DELIVERABLE 8: ACCELA CITIZEN ACCESS CONFIGURATION

This deliverable includes setup and configuration of the Patient Registry/Verification and Business Licensing web based access.

In terms of specific output, the following will be executed for this deliverable:

Our Responsibilities:

- Provide timely and appropriate responses to Agency's request for information.
- Setup Citizen Access branding by loading one banner file provided by the Agency
- Configure the citizen portal pages, based on Agency feedback, not to exceed 90 hours for this effort
- Accela is fixed-fee for up to 50 for Patient Registry/Verification
- Verify the loaded citizen access branding, citizen portal pages and sections updated and payment acceptance in environment, based on Agency feedback.

Agency Responsibilities:

- Provide timely and appropriate responses to Accela's requests for information.
- Provide website branding files, which include the top and side banner
- Arrange for the availability of appropriate Agency staff to review the branding on Citizen Access
- Agency staff must provide web branding
- Agency staff must review and test Patient Registry/Verification and Business Licensing web access configurations and provide feedback to Accela based on the agreed upon project plan timeline
- Any additional changes identified during review and testing beyond the scope identified above may be subject to a Change Order request
- Schedule appropriate Agency staff participants and meeting locations for activities.

Acceptance Criteria:

- Verify the operational Patient Registry/Verification and Business Licensing web access functionality such as login/logout, the updated citizen portal pages and sections, and payment acceptance

DELIVERABLE 9: ACCELA MOBILE APP CONFIGURATION

Accela will configure the Mobile Gateway for the Agency to utilize the Accela Mobile App for Cannabis Business Inspections and Enforcement activities. Accela will train Agency staff on the features of the Gateway and Agency Admin Portal.

In terms of specific output, the following will be executed for this deliverable:

- Accela Mobile App Sign On
- Demonstration of Agency Mobile Admin Portal to Agency Staff

Our Responsibilities:

- Set up Accela Mobile Gateway
- Configure Accela Mobile Gateway to work with Accela standard mobile devices

Acceptance Criteria:

- Login in to the Accela Mobile App under the Agency name

Acceptance Review Period:

Two (2) business days total

DELIVERABLE 10: REPORT CONFIGURATION

Accela will work with the agency to determine requirements, create specification documents and develop reports as needed to support the business process. Reports include tabular reports, letters, cards, licenses and any other printable output from the system. The reporting tools will include Cannabis-specific Standard Reports, Ad Hoc Report Writer, including making use of state provided reporting tools, such as SSRS, Crystal and PowerBI. Reports will only be developed once specification documents are approved by the agency.

Should the agency cancel a report requirement and work has already begun, then that report still counts against the hours.

In terms of specific output, the following will be executed for this deliverable:

- Report requirement analysis sessions
- Create report specifications
- Develop reports
- Demonstration of completed report in the development environment

Our Responsibilities:

- Work with Agency staff to identify reporting needs
- Create specifications for each report
- Develop reports to run from the Business Licensing systems
- Develop up to three (3) reports for the Patient Registry/Verifications (in accordance with HIPAA compliance)

Agency Responsibilities:

- Allocate the time for qualified business and technical experts for the report requirements sessions that are critical to the project success
- Review all specification documents within 2 business days

Acceptance Criteria:

- Review reports with sign-off from the Agency

DELIVERABLE 11: TRAINING

Accela will provide training for Agency staff that focuses on the administration, maintenance, and augmentation of the system Patient Registry/Verification and Business Licensing configurations. Accela aims to educate Agency resources on all aspects of all systems in an effort to ensure the Agency is self-sufficient.

All training will be delivered remotely. Should the agency request onsite training, all travel expenses will be reimbursed by the agency outside of this agreement with approval by the agency of all anticipated travel costs.

Accela will record any online training session and provide a copy.

In terms of specific output, the following will be executed for this deliverable:

- Accela Civic Platform Core Team Training (1 day)
- Accela Civic Platform Admin Usage (1 day) remote training
- Accela Civic Platform End User (Includes ACA Usage) (2 days), remote, up to 20 students
- Accela Ad-hoc Report training (0.5 day), remote training
- Supporting training documentation for End User Training
- Accela has allotted up to 88 hours for the Business Licensing Solution
- The Patient Registry/Verification is provided on a Fixed Fee basis. Includes direct training for system administrators. End users Training via train-the-trainer approach.

Our Responsibilities:

- Coordinate with the Agency to define training schedule and logistics.
- Deliver training per the specific requirements listed above.
- All training will be delivered remotely
- Online training sessions will be recorded and made available to the agency

Agency Responsibilities:

- Select and prepare the power-users who will be participating in the training and subsequently training end users.
- Arrange the time and qualified people for the training who are critical to the project success.
- Provide suitable Agency facilities to accommodate various training classes.
- Ensure that users are proficient in using PC's in a Windows environment as a prerequisite for the course.
- Ensure that users are familiar with use of standard Internet browsers as a prerequisite for the course.

Acceptance Criteria:

- Execution of training

DELIVERABLE 12: USER ACCEPTANCE TESTING (UAT)

Accela will assist the Agency to test and validate the solution and its readiness to be migrated to production for active use and will assist in transferring the solution and any required data from Support to Production as documented in all the deliverables.

Accela will provide support for training, oversight, answering questions and addressing issues discovered in User Acceptance Testing. It should be noted that it is critical that the Agency devote ample time and resources to this effort to ensure that the system is operating per as outlined in the deliverables and ready for the move to production. The Agency should test individual components of functionality of the solution (i.e., functional and/or unit testing), and also test to ensure that the interrelated parts of the Accela Civic Platform solution are operating properly (i.e., integration testing).

Accela will provide assistance to the Agency as needed by providing User Acceptance Testing (UAT) support and a defined testing process. We will address and rectify issues discovered during the UAT process as Agency staff executes testing activities. We will work with the Agency to develop a test plan, as well as an issue log to track the progress of testing. It should be noted that we will plan for a total of 1 week to complete this deliverable.

In terms of specific output, the following will be executed for this deliverable:

- Resolution of issues resulting from Agency User Acceptance Testing
- Fully tested system that is ready to move to production for go-live
- Accela has allotted up to 80 hours for Business Licensing
- Patient Registry/Verification is fixed fee up to 40 hours

Our Responsibilities:

- Provide recommendations on testing strategy and best practices.
- Lead the Agency in User Acceptance testing effort and the validation of the system configuration and its readiness to be migrated to production for active use.
- Resolution of issues as a result of User Acceptance Testing activities.

Agency Responsibilities:

- Provide timely and appropriate responses to Accela's requests for information.
- Make available the appropriate Agency key users and content experts to participate in user acceptance testing as defined and managed by Agency.
- Develop the User Acceptance test scripts.
- Utilize the use cases documented in each Configuration Document Deliverable as the basis for the acceptance of this Deliverable.

Acceptance Criteria:

- Completion of up to 80 hours of UAT for Business Licensing
- Patient Registry/Verification UAT is Fixed Fee

DELIVERABLE 13: POST DEPLOYMENT SUPPORT

We will work with the Agency to identify and address issues identified during this period using a Post Production Issues List. This list will be comprised of issues related to the defined deliverables listed in this SOW. Any additional items outside of the scope of the SOW may also be tracked at this stage.

The support period will last for 2 weeks from the go live date. At the end of the support period, Additionally, a formal meeting will be scheduled with the Agency and our team, for the purpose of transitioning future issues and questions from the Agency to the relevant support team.

In terms of specific output, the following will be executed for this deliverable:

- Post Deployment support will last for a period of 2 weeks with a not to exceed hourly allotment of 60 hours for Business Licensing.
- Post Deployment support for Patient Registry/Verification will last for a period of 2 weeks and hourly allotment is Fixed Fee.
- Transition of Agency from Services team to relevant support teams for ongoing support

Our Responsibilities:

- Support the agency Accela administrator for Accela developed configuration and components
- Assist with the identification of issues for the Post Production Issues List
- Assist with issues that may arise related to the deliverables in this SOW
- Transfer ongoing support of the client and to the Accela Support to address any post Production issues that require remediation

Agency Responsibilities:

- Provide technical and functional user support for post-production support and monitoring
- Develop and maintain a Post Production Issues List
- Provide timely and appropriate responses to requests for information

Acceptance Criteria:

- Up to 80 hours of support during a 2 week duration starting the day of go live

CONTINGENCY IMPLEMENTATION

Accela will work with the Agency to identify/recommend application of 120 hours for any use towards Business Licensing.

PROJECT MANAGEMENT

Assigned Project Managers from Accela will provide oversight on all implementation activities and report back to the Agency on status and progress. These Project Managers will be responsible for coordinating resources and meetings with the Agency.

Any delays in the original agreed upon schedule that are initiated by the Agency could result in an increase in scope of the project management activities.

In terms of specific output, the following will be executed for this deliverable:

Our Responsibilities:

- Conduct regular status meetings
- Coordinate all work activities and resources
- Maintain a regular cadence of status reporting
- Maintain the project schedule
- Establish a SharePoint environment to manage all project related activities and documentation

Acceptance Criteria:

- Completion of post go live support

Exhibit C
Bureau of Information and Telecommunications
Required Contract Terms

1.1 CONFIDENTIALITY OF INFORMATION:

For purposes of this paragraph, "State Proprietary Information" shall include all information disclosed to the Vendor by the State. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not disclose any State Proprietary Information to any third person for any reason without the express written permission of a State officer or employee with authority to authorize the disclosure. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall not: (i) disclose any State Proprietary Information to any third person unless otherwise specifically allowed under this agreement; (ii) make any use of State Proprietary Information except to exercise rights and perform obligations under this agreement; (iii) make State Proprietary Information available to any of its employees, officers, agents or third party Vendors except those who have a need to access such information and who have agreed to obligations of confidentiality at least as strict as those set out in this agreement. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities is held to the same standard of care in guarding State Proprietary Information as it applies to its own confidential or proprietary information and materials of a similar nature, and no less than holding State Proprietary Information in the strictest confidence. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall protect the confidentiality of the State's information from the time of receipt to the time that such information is either returned to the State or destroyed to the extent that it cannot be recalled or reproduced. The Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities agree to return all information received from the State to State's custody upon the end of the term of this agreement, unless otherwise agreed in a writing signed by both parties. State Proprietary Information shall not include information that:

- A. was in the public domain at the time it was disclosed to the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities;
- B. was known to the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction at the time of disclosure from the State;
- C. that was disclosed with the prior written approval of State's officers or employees having authority to disclose such information;
- D. was independently developed by the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities without the benefit or influence of the State's information;

- E. becomes known to the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities without restriction from a source not connected to the State of South Dakota.

State's Proprietary Information can include names, social security numbers, employer numbers, addresses and other data about applicants, employers or other clients to whom the State provides services of any kind. Vendor understands that this information is confidential and protected under State law. The parties mutually agree that neither of them nor any Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall disclose the contents of this agreement except as required by applicable law or as necessary to carry out the terms of the agreement or to enforce that party's rights under this agreement. Vendor acknowledges that the State and its agencies are public entities and thus may be bound by South Dakota open meetings and open records laws. It is therefore not a breach of this agreement for the State to take any action that the State reasonably believes is necessary to comply with South Dakota open records or open meetings laws.

1.2 CHANGE MANAGEMENT PROCESS:

From time to time it may be necessary or desirable for either the State or the Vendor to propose changes to the Services provided. Such changes shall be effective only if they are in writing and contain the dated signatures of authorized representatives of both parties. Unless otherwise indicated, a change or amendment shall be effective on the date it is signed by both parties. Automatic upgrades to any software used by the Vendor to provide any services that simply improve the speed, efficiency, reliability, or availability of existing services and do not alter or add functionality, are not considered "changes to the Services" and such upgrades will be implemented by the Vendor on a schedule no less favorable than that provided by the Vendor to any other customer receiving comparable levels of services.

1.3 WORK PRODUCTS:

The Vendor shall be responsible for the professional quality, technical accuracy, timely completion, and coordination of all services furnished by the Vendor and any subcontractors, if applicable, under this Agreement. It shall be the duty of the Vendor to assure that the services and the system are technically sound and in conformance with all pertinent Federal, State and local statutes, codes, ordinances, resolutions and other regulations. The Vendor shall, without additional compensation, correct or revise any errors or omissions in its work products.

Vendor hereby acknowledges and agrees that all State Proprietary Information, any information discovered by the State, Personally Identifiable Information (PII), data protected under Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax

Information (FTI) or any information defined under state statute as confidential, and all information contained therein provided to the State by the Vendor in connection with its performance under this Agreement shall belong to and is the property of the State and will not be used in any way by the Vendor without the written consent of the State.

1.4 CURING OF BREACH OF AGREEMENT:

In the event of a breach of these representations and warranties the State shall provide the Vendor with the opportunity to rectify the breach. The Vendor shall immediately, after notice from the State, begin work on curing such breaches. If the notice is telephonic the State will provide, at the Vendor's request, a written notice to reaffirm the telephonic notice. If such problem remains unaddressed after three days, Vendor will make reasonable efforts at Vendor's sole expense, to remedy the deficiency, failure, malfunction, defect, or problem. The rights and remedies provided in this paragraph are in addition to any other rights or remedies provided in this Agreement or by law.

1.5 DOMAIN NAME OWNERSHIP:

Any website(s) that the Vendor creates as part of this project must have the domain name registered by and owned by the State. If as part of this project the Vendor is providing a service that utilizes a website with the domain name owned by the Vendor, the Vendor must give thirty (30) days' notice before abandoning the site. If the Vendor intends to sell the site to another party the Vendor must give the State thirty days (30) notice and grant the State the right of first refusal. For any site or domain, whether hosted by the Vendor or within the State web infrastructure, any and all new web content should first be created in a development environment and then subjected to security scan before being approved for a move up to the production level.

1.6 SOFTWARE FUNCTIONALITY AND REPLACEMENT:

The software licensed by the Vendor to the State provides the following functionality:

The solution will be used to register and verify medical marijuana patients and designated caregivers. It will also be used to register medical marijuana businesses and to manage the necessary interactions between the state and applicants/registrant businesses.

The Vendor agrees that:

- A. If in the opinion of the State the Vendor reduces or replaces the functionality contained in the licensed product and provides this functionality as a separate or

renamed product, the State shall be entitled to license such software product at no additional license or maintenance fee.

- B. If in the opinion of the State the Vendor releases an option, future product, purchasable product or other release that has substantially the same functionality as the software product licensed to the State, and it ceases to provide maintenance for the older software product, the State shall have the option to exchange licenses for such replacement product or function at no additional charge. This includes situations where the Vendor discontinues the licensed product and recommends movement to a new product as a replacement option regardless of any additional functionality the replacement product may have over the licensed product.

1.7 LICENSE GRANT:

- A. Subject to the terms and conditions set forth in Exhibit A-1 herein, the Vendor grants to the State a worldwide, nonexclusive license to use the software and associated documentation, plus any additional software which shall be added by mutual agreement of the parties during the term of this agreement.
- B. The license usage model is based on a future known number of internal state users that will fluctuate over time, an unknown number of external public users that cannot reasonably be predicted, and an unknown number of external law enforcement users that will fluctuate and cannot be predicted at any given time.
- C. The license grant may be extended to any Authorized Users, as defined in Exhibit A-1, who have a need to use the software for the benefit of the State.

1.8 FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:

The Parties agree that the State shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto. The State also maintains its termination privileges if the Vendor enters bankruptcy.

1.9 DATA RECOVERY:

The Consultant must be able to recover the State's data in the same state it was sent to the Consultant for 13 months. If the Consultant system or the third-party system that is hosting data for the Consultant is subjected to a disaster severe enough to implement disaster recovery procedures, then recovery of the State data will follow the disaster recovery requirements for Recovery Time Objective and Recovery Point Objective agreed to by the State and the Consultant.

1.9.1 REJECTION OR EJECTION OF VENDOR, AND VENDOR'S SUBCONTRACTORS, AGENTS, ASSIGNS AND/OR AFFILIATED ENTITIES EMPLOYEE(S):

The State, at its option, may require the vetting of the Vendor, and any of the Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities. The Vendor is required to assist in this process as needed.

With the exception of the entities identified in Attachment C-1, The State reserves the right to reject any person from participating in the project or require the Vendor to remove from the project any person the State believes is detrimental to the project or is considered by the State to be a security risk. The State will provide the Vendor with notice of its determination, and the reasons for the rejection or removal if requested by the Vendor. If the State signifies that a potential security violation exists with respect to the request, the Vendor shall immediately remove the individual from the project.

1.10 THREAT NOTIFICATION:

Upon becoming aware of a credible security threat with the Vendor's product(s) and or service(s) being used by the State, the Vendor or any subcontractor supplying product(s) or service(s) to the Vendor needed to fulfill the terms of this Agreement will notify the State within two (2) business days of any such threat. If the State requests, the Vendor will provide the State with information on the threat. A credible security threat consists of the discovery of an exploit that a person considered an expert on Information Technology security believes could be used to breach one or more aspects of a system that is holding State data, or a product provided by the Vendor.

1.11 SECURITY INCIDENT NOTIFICATION:

For protected non-health information only, the Vendor will implement, maintain, and update Security Incident procedures that comply with all State standards and Federal and State requirements. A Security Incident is a violation of any BIT security or privacy policies or contract agreements involving sensitive information, or the imminent threat of a violation. The BIT security policies can be found in the Information Technology Security Policies found at: <https://bit.sd.gov/vendor/default.aspx>. The State requires notification of a Security Incident involving any of the State's sensitive data in the Contractor's possession. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute Security Incidents, this Agreement constitutes notice by Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, as long

as such probes and reconnaissance scans do not result in a Security Incident as defined above. Except as required by other legal requirements the Vendor shall only provide notice of the incident to the State. The State will determine if notification to the public will be by the State or by the Vendor. The method and content of the notification of the affected parties will be coordinated with, and is subject to approval by the State, unless required otherwise by legal requirements. If the State decides that the Vendor will be distributing, broadcasting to or otherwise releasing information on the Security Incident to the news media, the State will decide to whom the information will be sent, and the State must approve the content of any information on the Security Incident before it may be distributed, broadcast or otherwise released. The Vendor must reimburse the State for any costs associated with the notification, distributing, broadcasting or otherwise releasing information on the Security Incident.

- A. The Vendor shall notify the State Contact within twenty-four (24) hours of the Vendor becoming aware that a Security Incident has occurred.
If notification of a Security Incident to the State Contact is delayed because it may impede a criminal investigation or jeopardize homeland or federal security, notification must be given to the State within twenty-four (24) hours after law-enforcement provides permission for the release of information on the Security Incident.
- B. Notification of a Security Incident at a minimum is to consist of the nature of the data exposed, the time the incident occurred and a general description of the circumstances of the incident. If not all of the information is available for the notification within the specified time period Vendor shall provide the State with all of the available information along with the reason for the incomplete notification. A delay in excess of twenty-four (24) hours is acceptable only if it is necessitated by other legal requirements.
- C. At the State's discretion, the Vendor must provide to the State all data available including: (i) Name of and contact information for the Vendor's Point of Contact for the Security Incident; (ii) date and time of the Security Incident; (iii) date and time the Security Incident was discovered; (iv) description of the Security Incident including the data involved, being as specific as possible; (v) the potential number of records, and if unknown the range of records; (vi) address where the Security Incident occurred; and, (vii) the nature of the technologies involved. Notifications must be sent electronically and encrypted via NIST or other applicable federally approved encryption techniques. If there are none, use AES256 encryption. Vendor shall use the term "data incident report" in the subject line of the email. If not all of

the information is available for the notification within the specified time period Vendor shall provide the State with all of the available information along with the reason for the incomplete information. A delay in excess of twelve (12) hours is acceptable only if it is necessitated by other legal requirements.

- D. If the information from the Breach of System Security includes State of South Dakota residents whose personal or protected information was, or is reasonably believed to have been, acquired by an unauthorized person Vendor must notify the resident(s) in accordance with South Dakota Codified Law (SDCL) Chapter 22-40. Requirements of this chapter include that if there are two-hundred and fifty (250) or more residents' records involved the State of South Dakota Attorney General (ATG) must be notified. Both notifications must be within sixty (60) days of the discovery of the breach. The Vendor shall also notify, without unreasonable delay, all consumer reporting agencies, as defined under 15 U.S.C. § 1681a in effect as of January 1, 2018, and any other credit bureau or agency that compiles and maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notice. The Vendor is not required to make a disclosure under this section if, following an appropriate investigation and notice to the ATG, the Vendor reasonably determines that the breach will not likely result in harm to the affected person. The Vendor shall document the determination under this section in writing and maintain the documentation for not less than three (3) years. These statements of requirements from SDCL 22-40 are neither comprehensive nor all inclusive, and Vendor shall comply with all applicable provisions of that chapter.

The requirements of section D do not replace the requirements of sections A, B and C but are in addition to them.

1.12 HANDLING OF SECURITY INCIDENT:

For Security Incidents of protected non-health information under the Vendor's control and at the State's discretion the Vendor will preserve all evidence regarding a security incident including but not limited to communications, documents, and logs. The Vendor will also:

- A. fully investigate the incident,
- B. cooperate fully with the State's investigation of, analysis of, and response to the incident,
- C. make a best effort to implement necessary remedial measures as soon as it is possible and,

- D. document responsive actions taken related to the Security Incident, including any post-incident review of events and actions taken to implement changes in business practices in providing the services covered by this agreement.

If the Security Incident was directly and exclusively attributable to the actions or inactions of the Vendor, the Vendor will, at the Vendor's sole expense, use a credit monitoring service, call center, forensics company, advisors, or public relations firm as needed to offer one (1) year of credit monitoring to each person whose data was compromised. The State will set the scope of any investigation. The State can require a risk assessment for which the Vendor, the State will mandate the methodology and the scope. At the State's discretion a risk assessment may be performed by a third party at the Vendor's expense.

If the Vendor is required by federal law or regulation to conduct a Security Incident or data breach investigation, the results of the investigation must be reported to the State within twenty-four (24) hours of the investigation report being completed. If the Vendor is required by federal law or regulation to notify the affected parties, the State must also be notified, unless otherwise required by law.

Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the State under law or equity, the Vendor will reimburse the State in full for all costs incurred by the State in investigation and remediation of the Security Incident including, but not limited, to providing notification to regulatory agencies or other entities as required by law or contract. The Vendor shall also pay all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident.

1.13 SECURITY INCIDENTS REGARDING PROTECTED HEALTH INFORMATION:

Security Incident means the successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as defined in 45 CFR 164.304. "Security Incident" also includes the unauthorized use of system privileges, unauthorized access to State data, execution of malware, physical intrusions and electronic intrusions that may include network, applications, servers, workstations and social engineering of staff. The Vendor shall alert the State Contact within twenty-four (24) hours of a Security Incident and provide daily updates to the BIT contact at their request. The Parties agree that this alert does not affect the Vendor's obligations under the Business Associate Agreement or the requirements of 45 CFR 164.410. The parties agree that, to the extent probes and reconnaissance scans common to the industry constitute a Security Incident, this Agreement constitutes notice by Vendor of the ongoing existence and occurrence of such Security Incidents for which no additional notice to the State shall be required. Probes and

scans include, without limitation, pings and other broadcast attacks in the Vendor's firewall, port scans, and unsuccessful log-on attempts, as long as such probes and reconnaissance scans do not result in a Security Incident as defined above. The State can require the Vendor to conduct a review or investigation within the scope and methodology determined by the State. At the State's discretion, the review or investigation may be performed by a third party at the Vendor's expense.

Notwithstanding any other provision of this Agreement and in addition to any other remedies available to the State under law or equity, in the event the investigation or review determines that the Vendor is responsible for the Security Incident, and where the State incurs any costs in the investigation, review or remediation of the Security Incident, the Vendor shall reimburse the State in full for all such costs. Costs include, but are not limited to, providing notification to regulatory agencies or other entities as required by law or contract. In the event the investigation or review determines that the Vendor is responsible for the Security Incident, the Vendor shall also pay any and all legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Incident, and all costs associated with the remediation of the Vendor's services and/or product(s).

1.14 ADVERSE EVENT:

Reserved.

1.15 BROWSER:

The system, site, and/or application must be compatible with vendor supported versions of Edge, Chrome, Safari, and Firefox browsers. Silverlight, QuickTime, PHP, and Adobe Flash will not be used in the system, site, and/or application. Adobe Animate CC is allowed if files that require third-party plugins are not required.

1.16 SECURITY ACKNOWLEDGEMENT FORM:

The Vendor will be required to sign the Security Acknowledgement form which is attached to this Agreement as Exhibit D. The signed Security Acknowledgement form must be submitted to the State and approved by the South Dakota Bureau of Information and Telecommunications and communicated to the Vendor by the State contact before work on the contract may begin. This form constitutes the agreement of Vendor to be responsible and liable for ensuring that the Vendor, Vendor's employee(s), and Subcontractor's, Agents, Assigns and or Affiliated Entities and all of their employee(s), participating in the work will abide by the terms of the Information Technology Security Policy- Contractor Version (ITSP) found at <https://bit.sd.gov/vendor/default.aspx> . Failure to abide by the requirements of the ITSP or the Security Acknowledgement form can be considered a breach of this Agreement at the

discretion of the State. It is also a breach of this Agreement, at the discretion of the State, if the Vendor does not sign another Security Acknowledgement form covering any employee(s) and any Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s), any of whom are participating in the work covered by this Agreement, and who begin working under this Agreement after the project has begun. Any disciplining of the Vendor's, Vendor's employee(s) or Subcontractor's, Agents, Assigns and or Affiliated Entities employee(s) due to a failure to abide by the terms of the Security Acknowledgement Form will be done at the discretion of the Vendor or Subcontractor's, Agents, Assigns and or Affiliated Entities and in accordance with the Vendor's or Subcontractor's, Agents, Assigns and or Affiliated Entities personnel policies. Regardless of the actions taken by the Vendor and Subcontractor's, Agents, Assigns and or Affiliated Entities, the State shall retain the right to require at its discretion the removal of the employee(s) from the project covered by this agreement.

1.17 BACKGROUND CHECKS:

The State requires all employee(s) of the Vendor, Subcontractors, Agents, Assigns and or Affiliated Entities who write or modify State owned software, alter hardware, configure software of state-owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas to undergo fingerprint-based background checks. These fingerprints will be used to check the criminal history records of both the State and the Federal Bureau of Investigation. These background checks must be performed by the State with support from the State's law enforcement resources. The State will supply the fingerprint cards and prescribe the procedure to be used to process the fingerprint cards. Project plans should allow two (2) to four (4) weeks to complete this process. If work assignments change after the initiation of the project covered by this agreement so that employee(s) of the Vendor, Subcontractor's, Agents, Assigns and or Affiliated Entities will be writing or modifying State owned software, altering hardware, configuring software of state owned technology resources, have access to source code and/or protected personally identifiable information or other confidential information or have access to secure areas then, background checks must be performed on any employees who will complete any of the referenced tasks. The State reserves the right to require the Vendor to prohibit any employee, Subcontractors, Agents, Assigns and or Affiliated Entities from performing work under this Agreement whenever the State, in its sole discretion, believes that having a specific employee, subcontractor, agent assign or affiliated entity performing work under this Agreement is detrimental to the project or is considered by the State to be a security risk, based on the results of the background check. The State will provide the Vendor with notice of this determination.

1.18 INFORMATION TECHNOLOGY STANDARDS:

Any service, software or hardware provided under this agreement will comply with state standards which can be found at <http://bit.sd.gov/standards/>

1.19 SECURITY:

The Vendor shall take all actions necessary to protect State information from exploits, inappropriate alterations, access or release, and malicious attacks. By signing this agreement, the Vendor warrants that:

- A. All Critical, High, Medium, and Low security issues are resolved. Critical, High and Medium can be described as follows:
 - A. **Critical** - Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices.
 - B. **High** - The vulnerability is difficult to exploit; however, it is possible for an expert in Information Technology. Exploitation could result in elevated privileges.
 - C. **Medium** - Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. Denial of service vulnerabilities that are difficult to set up.
 - D. **Low**- Vulnerabilities identified by the State as needing to be resolved that are not Critical, High, or Medium issues.
- B. Assistance will be provided to the State by the Vendor in performing an investigation to determine the nature of any security issues that are discovered or are reasonably suspected after acceptance. The Vendor will fix or mitigate the risk based on the following schedule: Critical and high risk, within 7 days, medium risk within 14 days, low risk, within 30 days.
- C. State technology standards, policies, and best practices will be followed. State technology standards can be found at <http://bit.sd.gov/standards/>.
- D. All members of the development team have been successfully trained in secure programming techniques.
- E. A source code control system will be used that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.
- F. State access to the source code will be allowed to ensure State security standards, policies, and best practices which can be found at <http://bit.sd.gov/standards/>.
- G. The Vendor will fully support and maintain the Vendor's application on platforms and code bases (including but not limited to: operating systems, hypervisors, web presentation layers, communication protocols, security products, report writers, and any other technologies on which the application depends) that are still being supported, maintained, and patched by the applicable third parties owning them. The Vendor may not withhold support from the State for this application nor

charge the State additional fees as a result of the State moving the Vendor's application to a new release of third-party technology if:

- a. The previous version of the third-party code base or platform is no longer being maintained, patched, and supported; and
- b. The new version to which the State moved the application is actively maintained, patched, and supported.

If there are multiple versions of the applicable code base or platform(s) supported by the third party in question, the Vendor may limit their support and maintenance to any one or all of the applicable third-party code bases or platforms.

If a code base or platform on which the Vendor's application depends is no longer supported, maintained, or patched by a qualified third party the Vendor commits to migrate its application from that code base and/or platform to one that is supported, maintained, and patched after the State has performed a risk assessment using industry standard tools and methods. Failure on the part of the Vendor to work in good faith with the State to secure or a timely move to supported, maintained, and patched technology will allow the State to cancel this Agreement without penalty.

1.20 MALICIOUS CODE:

- A. The Vendor warrants that the service/ licensed software contains no code that does not support an application requirement.
- B. The Vendor warrants that the service/ licensed software contains no malicious code.
- C. The Vendor warrants that the Vendor will not insert into the service/ licensed software or any media on which the service/ licensed software is delivered any malicious or intentionally destructive code.
- D. The Vendor warrants that the Vendor will use commercially reasonable efforts consistent with industry standards to scan for and remove any malicious code from the service/ licensed software before installation. In the event any malicious code is discovered in the service/ licensed software delivered by the Vendor, the Vendor shall provide the State at no charge with a copy of the applicable service/ licensed software that contains no malicious code or otherwise correct the affected portion of the services provided to the State. The remedies in this paragraph are in addition to other additional remedies available to the State.

1.21 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD:

Any service provider who possesses or interacts with payment card data must stay current with the Payment Card Industry (PCI) Data Security Standards. The Vendor shall enter into a contract with one or more service providers for payment card services under this Agreement. The Vendor shall provide to the State a written acknowledgement from any such service provider with whom the Vendor contracts for such services under this Agreement which acknowledgement shall state that the service provider is committed to maintaining proper security of the payment card data in its possession and is responsible for the security of payment card data the service provider possesses or otherwise stores, processes, or transmits on behalf of the Vendor. The Vendor must ensure that the service provider(s) used by the Vendor meet the Payment Card Industry Data Security Standards. The Vendor will annually review the service provider(s) policies and procedures and supporting documentation. The State at its discretion, can require the Vendor to provide the State with an annual report on the status of compliance of their service provider(s) with the Payment Card Industry Data Security Standards.

1.22 PAYMENT CARD INDUSTRY QUALIFICATION REQUIREMENTS FOR QUALIFIED INTEGRATORS AND RESELLERS:

When having a payment card application implemented, configured and or supported the Vendor and any subcontractor(s) used by the Vendor to fulfil the terms of this contract will have successfully met the Payment Card Industry qualification requirements for Qualified Integrators and Resellers (QIR). Should the Vendor or any subcontractor(s) used by the Vendor have their QIR revoked or fail to maintain their QIR the Vendor must immediately cease trying to implement, configuring and or supporting payment card application(s) required by the terms of this Agreement and inform the State Contact. At the State's discretion the Agreement may be terminated without any further obligation of the State.

1.23 LICENSE AGREEMENTS:

Vendor warrants that it has provided to the State and incorporated into this Agreement all license agreements, End User License Agreements, and terms of use regarding its software or any software incorporated into its software before execution of this Agreement. Failure to provide all such license agreements, End User License Agreements (EULA), and terms of use shall be a breach of this Agreement at the option of the State. The parties agree that neither the State nor its end_users shall be bound by the terms of any such agreements not timely provided pursuant to this paragraph and incorporated into this Agreement. Any changes to the terms of this Agreement or any additions or subtractions must first be agreed to by both parties in writing before they go into effect. This paragraph shall control and supersede the language of any such agreements to the contrary.

1.24 WEB AND MOBILE APPLICATION:

The Vendor's application is required to;

- A. have no code or services including web services included in or called by the application unless they provide direct, functional requirements that support the State's business goals for the application;
- B. encrypt data in transport and at rest using a mutually agreed upon encryption format;
- C. close all connections and close the application at the end of processing;
- D. the documentation will be in grammatically complete text for each call and defined variables (Use no abbreviations and use complete sentences, for example.) sufficient for a native speaker of English with average programming skills to determine the meaning and/or intent of what is written without prior knowledge of the application.
- E. have no code not required for the functioning of application;
- F. have no "back doors", a back door being a means of accessing a computer program that bypasses security mechanisms, or other entries into the application other than those approved by the State;
- G. permit no tracking of device user's activities without providing a clear notice to the device user and requiring the device user's active approval before the application captures tracking data;
- H. have no connections to any service not required by the functional requirements of the application or defined in the project requirements documentation;
- I. fully disclose in the "About" information that is the listing of version information and legal notices, of the connections made, permission(s) required, and the purpose of those connections and permission(s);
- J. ask only for those permissions and access rights on the user's device that are required for the defined requirements of the Vendor's application;
- K. access no data outside what is defined in the "About" information for the Vendor's application;
- L. your web site application produced for the State must conform to Web Content Accessibility Guidelines 2.0;
- M. any website developed for the State and hosted by the State must have a Single Sign On capability with the State's other websites;
- N. if any health or medical information is gathered or accessed by this application that is not protected by HIPAA and HITECH rules and regulations then the opening screen must state, in an easy to read font that the application is gathering and or accessing

health and or medical information and the user's privacy is not protected by federal regulations; and

O. any application to be used on a mobile device must be password protected.

The Vendor is required to disclose all:

- A. functionality;
- B. device and functional dependencies;
- C. third party libraries used;
- D. methods user data is being stored, processed or transmitted;
- E. methods used to notify the user how their data is being stored, processed and or transmitted;
- F. positive actions required by the user to give permission for their data to be stored, processed and or transmitted;
- G. methods used to record the user's response(s) to the notification that their data is being stored, processed and or transmitted;
- H. methods used to secure the data in storage, processing or transmission; and
- I. forms of authentication required for a user to access the application or any data it gathers stores, processes and or transmits;
- J. methods used to create and customize existing reports;
- K. methods used to integrate with external data sources;
- L. methods used if integrates with public cloud provider;
- M. methods and techniques used and the security features that protect data, if a public cloud provider is used; and
- N. formats the data and information uses.

If the application does not adhere to the requirements given above or the Vendor has unacceptable disclosures, at the State's discretion, the Vendor will rectify the issues at no cost to the State.

1.25 INTENDED DATA ACCESS METHODS:

The Vendor's application will not allow a user, external to the State's domain, to bypass logical access controls required to meet the application's functional requirements. All database queries using the Vendor's application can only access data by methods consistent with the intended business functions.

If the State can demonstrate the application flaw, to the State's satisfaction, then the Vendor will rectify the issue, to the State's satisfaction, at no cost to the State

1.26 OFFSHORE SERVICES:

The Vendor will not provide access to State data to any entity or person(s) located outside the continental United States that are not named in this Agreement without the written permission of the State. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States.

1.27 VENDOR'S SOFTWARE LICENSES:

The Vendor must disclose to the State the license(s) for any third-party software and libraries used by the Vendor's product(s) ((and/or) in the project by the Vendor) covered under this agreement if the State will not be the license(s) holder. The Vendor is required to provide copies of the license(s) for the third-party software and libraries to the State. No additional software and libraries may be added to the project after the contract is signed without notifying the State and providing the licenses of the software and libraries. Open source software and libraries are also covered by this clause. Any validation of any license(s) used by the Vendor to fulfil the Vendor's commitments agreed to in this agreement is the responsibility of the Vendor, not the State.

1.28 VENDOR TRAINING REQUIREMENTS:

The Vendor, Vendor's employee(s), and Vendor's Subcontractors, Agents, Assigns, Affiliated Entities and their employee(s), must successfully complete, at the time of hire and annually thereafter, a cyber-security training program. The training must include but is not limited to: i) Legal requirements for handling data, ii) Media sanitation, iii) Strong password protection, iv) Social engineering, or the psychological manipulation of persons into performing actions that are inconsistent with security practices or that cause the divulging of confidential information, v) Security incident response, and vi) Protected Health Information.

1.29 DATA SANITIZATION:

At the end of the project covered by this Agreement the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities shall return the State's data and/or securely dispose of all State data in all forms, this can include State data on media such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. This State data must be permanently deleted by either purging the data or destroying the medium on which the State data is found according to the methods given in the most current version of NIST 800-88. Certificates of Sanitization for Offsite Data (See bit.sd.gov/vendor/default.aspx for copy of certificate) must be completed by the Vendor and given to the State Contact. The State will review the completed Certificates of Sanitization for Offsite Data. If the State is not satisfied by the data sanitization then the Vendor will use a process and procedure that does satisfy the State. The only exceptions are when the State Data must be maintained after the project is completed for legal reasons or the State data is on a backup medium where the State data

cannot be separated from other data. If the state data cannot be sanitized for these reasons, then the Vendor must encrypt the data to at least 256 AES with SHA 2 or SHA 256 hashing and maintain the medium in a facility that meets the security requirements of the most current version of NIST 800-53 or IRS 1075 whichever is relevant.

This contract clause remains in effect for as long as the Vendor, and Vendor's Subcontractors, Agents, Assigns and/or Affiliated Entities have the State data, even after the Agreement is terminated or the project is completed.

1.30 BANNED HARDWARE:

The Vendor will not provide to the State any computer hardware or video surveillance hardware, or any components thereof, or any software that was manufactured, provided, or developed by a covered entity. As used in this paragraph, "covered entity" means the following entities and any subsidiary, affiliate, or successor entity and any entity that controls, is controlled by, or is under common control with such entity: Kaspersky Lab, Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, or any entity that has been identified as owned or controlled by, or otherwise connected to, People's Republic of China. The Vendor will immediately notify the State if the Vendor becomes aware of credible information that any hardware, component, or software was manufactured, provided, or developed by a covered entity.

1.31 USE OF PORTABLE DEVICES:

The Vendor shall prohibit its employees, agents, affiliates, and subcontractors from storing State data on portable devices, including personal computers, except for devices that are used and kept only at the Vendor's data center(s). All portable devices used for storing State Data must be password protected and encrypted.

1.32 REMOTE ACCESS:

The Vendor shall prohibit its employees, agents, affiliates, and subcontractors from accessing State data remotely except as necessary to provide the services under this Agreement and consistent with all contractual and statutory requirements. The accounts used for remote access cannot be shared accounts and must include multifactor authentication.

1.33 VENDOR ELECTION NOT TO RENEW CONTRACT OR TO INCREASE FEES:

The Vendor is obligated to give the State one hundred and eighty (180) days written notice in the event the Vendor intends not to renew the contract or intends to raise any fees or costs associated

with the Vendor's products or services in a subsequent contract unless such fees or costs have previously been negotiated and included in this contract.

1.34 PROVISION OF DATA:

Upon notice of termination by either party, the State will be provided by the Vendor all current State Data in a non-proprietary form. Upon the effective date of the termination of the agreement, the State will again be provided by the Vendor with all current State Data in a non-proprietary form. State Data is any data produced or provided by the State as well as any data produced or provided for the State by a third-party.

1.35 DATA LOCATION:

The Vendor shall provide its services to the State as well as storage of State data solely from data centers in the continental United States. The Vendor will not allow any State to be provided to or accessed by any entity outside the continental United States. This restriction includes but is not limited to Vendor's employees and contractors. This restriction also applies to disaster recovery; any disaster recovery plan must provide for data storage entirely within the continental United States. The Vendor shall not allow its employees or contractors to store State data on portable devices, including personal computers, except for devices that are used and kept only at its data centers. The Vendor shall permit its personnel and contractors to access State data remotely only as required to provide technical support or to fulfill the terms of this Agreement. If the State's data being remotely accessed is legally protected data or considered sensitive by the State, then:

- A. The device used must be password protected;
- B. Multifactor Authentication must be used;
- C. The data is encrypted to at least AES 256 both in transit and in storage;
- D. Data is not put onto mobile media;
- E. No non-electronic copies are made of the data;
- F. The Vendor maintains a log on what data was accessed, when it was accessed, and by whom it was accessed;

The State's Data Sanitization policies are to be followed when the data is no longer needed on the device used to access the data remotely.

1.36 DATA PROTECTION:

Protection of personal privacy and data shall be an integral part of the business activities of the Vendor to ensure there is no inappropriate or unauthorized use of State's data at any time. To this end, the Vendor shall safeguard the confidentiality, integrity and availability of State's data and comply with the following conditions:

- A. The Vendor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personally Identifiable Information (PII), data protected under the Family Educational Rights and Privacy Act (FERPA), Protected Health Information (PHI), Federal Tax Information (FTI) or any information that is confidential under state law. Such security measures shall be in accordance with recognized industry practice and not less protective than the measures the Vendor applies to its own non-public data.
- B. At no time shall any data that either belong to or are intended for the use of the State or its officers, agents or employees — be copied, disclosed or retained by the Vendor or any party related to the Vendor for subsequent use in any transaction that does not include the State.
- C. The Vendor will not use such data for the Vendor's own benefit and, in particular will not engage in data mining of State's data or communications, whether through automated or manual means, except as specifically and expressly required by law or authorized in writing by the State through a State employee or officer specifically authorized to grant such use of State data.

1.37 INDEPENDENT AUDIT:

The Vendor will disclose any independent audits that are performed on any of its systems. The systems included under this requirement are the Vendor's data center. This information on an independent audit(s)-shall be provided to the State in any event, whether the audit or certification process is successfully completed or not. The audit shall also be disclosed if the audit process did not result in a positive outcome. The Vendor will provide a copy of the findings of the audit(s) to the State.

1.38 NON-DISCLOSURE AND SEPARATION OF DUTIES:

The Vendor shall enforce separation of job duties and require non-disclosure agreements of all staff that have or can have access to State data or the hardware that State data resides on. The Vendor will limit staff knowledge to those staff who duties that require them to have access to the State's data or the hardware the State's data resides on.

1.39 BUSINESS CONTINUITY AND DISASTER RECOVERY:

The Vendor shall provide a business continuity and disaster recovery plan upon request and ensure that the State's Recovery Time Objective (RTO) of twelve (12) hours and Recovery Point objective (RPO) of three (3) days is met. For purposes of this contract, a "Disaster" shall mean

any unplanned interruption of the operation of or inaccessibility to the Vendor's service in which the State, using reasonable judgment, requires relocation of processing to a recovery location. The State shall notify the Vendor as soon as possible after the State deems a service outage to be a Disaster.

1.40 STOLEN DATA LIABILITY:

In no event shall the Vendor be liable for loss of good will, or for special, indirect, incidental, consequential or punitive damages arising from the state's use of the services of the Vendor, regardless of whether such claim arises in tort or in contract.

If the state's records or other data submitted for processing are lost or damaged as a result of any failure by the Vendor, its employees or agents to exercise reasonable care to prevent such loss or damages the Vendor's liability on account of such loss or damages shall not exceed the reasonable cost of reproducing such records or data. This limitation shall not apply in the event that the records or data cannot be reproduced at reasonable cost.

1.41 EXTRACTION OF DATA:

Upon notice of termination by the Vendor or upon reaching the end of the term, any information stored in repositories not hosted on the State's infrastructure shall be extracted in a format to enable to State to load the information onto\into repositories. If this is not possible the information metadata, including data structure descriptions and data dictionary, and data will be extracted into a text file format and returned to the State. Upon the effective date of the termination of the agreement the State again requires that State applications that store information to repositories not hosted on the State's infrastructure require the Vendor before termination (whether initiated by the State or the Vendor) to extract the State's information such that the state is able to load the information onto or into repositories listed in the State's standards. If the information cannot be extracted in a format that allows the information to be loaded onto or into the State's Standard repositories the information (metadata (data structure descriptions) and data) will be extracted into a text file format and returned to the State. The Vendor recognizes and agrees that the State cannot enter into an agreement providing for hosting of any of its data on the Vendor's servers and networks without provisions protecting its ability to access and recover its data in a usable, non-proprietary format in the event of termination of this contract with sufficient time to convert that data and the business functions provided by the Vendor to another system and Vendor.

1.42 RIGHTS AND LICENSE IN AND TO STATE DATA:

The parties agree that between them, all rights including all intellectual property rights in and to State's data shall remain the exclusive property of the State, and that the Vendor has a

limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder. This Agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

1.43 CESSATION OF BUSINESS:

The Vendor will notify the State of impending cessation of its business or that of a tiered provider and the Vendor's contingency plan. This plan should include the immediate transfer of any previously escrowed assets and data and State access to the Vendor's facilities to remove or destroy any State-owned assets and data. The Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the State. The Vendor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its services and those to be provided by its successor. The Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to the State. The Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and impact on the State, all such work to be coordinated and performed in advance of the formal, final transition date.

1.44 LEGAL REQUESTS FOR DATA:

Except as otherwise expressly prohibited by law, the Vendor will:

- A. Immediately notify the State of any subpoenas, warrants, or other legal orders, demands or requests received by the Vendor seeking State data maintained by the Vendor;
- B. Consult with the State regarding its response;
- C. Cooperate with the State's requests in connection with efforts by the State to intervene and quash or modify the legal order, demand or request; and
- D. Upon the State's request, provide the State with a copy of both the demand or request and its proposed or actual response.

1.45 EDISCOVERY:

The Vendor shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Vendor shall not respond to service of process, and other legal requests related to the State without first notifying the State unless prohibited by law from providing such notice.

1.46 DATA RETENTION AND DISPOSAL:

- A. Using appropriate and reliable storage media, the Vendor will regularly back up State's data and retain such backup copies for a minimum of 36 months.
- B. The Vendor will retain logs associated with End User activity for a minimum of 7 years unless the parties mutually agree to a different period.

1.47 ACCESS ATTEMPTS:

All access attempts, whether failed or successful, to any system connected to the hosted system which can access, read, alter, intercept, or otherwise impact the hosted system or its data or data integrity shall be logged by the Vendor. For all systems, the log must include at least: log-in page used, username used, time and date stamp, incoming IP for each authentication attempt, and the authentication status, whether successful or not. Logs must be maintained not less than 7 years in a searchable database in an electronic format that is un-modifiable. At the request of the state, access must be granted to search those logs as needed to demonstrate compliance with the terms of this contract, and any and all audit requirements related to the hosted system.

1.48 PASSWORD POLICIES:

Password policies for all Vendor employees will be documented and provided to the state to assure adequate password protections are in place. Logs and administrative settings will be provided to the state on request to demonstrate such policies are actively enforced. The process used to reset a password must include security questions or Multifactor Authentication.

1.49 ANNUAL RISK ANALYSIS:

The Vendor will conduct a risk analysis annually or when there has been a significant system change. The Vendor will provide verification to the State Contact upon request that the risk analysis has taken place. At a minimum the risk analysis will include a review of the:

- A. Penetration testing of the Vendor's system.
- B. Security policies and procedures.
- C. Disaster recovery plan.
- D. Security incident plan.
- E. Business Associates Agreements.
- F. Inventory of physical systems, devices and media that store or utilize ePHI for completeness.

If the risk analysis provides evidence of deficiencies a risk management plan will be produced. A summary of the risk management plan will be sent to the State Contact. The summary will

include completion dates for the plan's milestones. Updates on the risk management plan will be sent to the State Contact upon request.

1.50 ACCESS TO STATE DATA:

Unless this Agreement is terminated, State access to State data amassed under the project covered by this Agreement will not be hindered if there is a:

- A. Contract dispute between the parties to this Agreement.
- B. There is a billing dispute between the parties to this Agreement.
- C. The Vendor merges with or is acquired by another company.

The Vendor will also maintain all security requirements of the State as well as any disaster recovery commitments made under this Agreement.

1.51 THIRD PARTY HOSTING:

If the Vendor has the State's data hosted by another party the Vendor must provide the State, the name of this party. The Vendor must provide the State with contact information for this third party and the location of their data center(s). The Vendor must receive from the third party written assurances that the state's data will reside in the continental United States at all times and provide these written assurances to the State. This restriction includes the data being viewed or accessed by the third-party's employees or contractors. If during the term of this agreement the Vendor changes from the Vendor hosting the data to a third-party hosting the data or changes third-party hosting provider, the Vendor will provide the State with one hundred and eighty (180) days' advance notice of this change and at that time provide the state with the information required above.

1.52 SECURING OF DATA:

All facilities used to store, and process State's data will employ industry best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure the Vendor's own data of a similar type, and in no event less than commercially reasonable in view of the type and nature of the data involved. Without limiting the foregoing, the Vendor warrants that all State's data will be encrypted in transmission (including via web interface) and storage at no less than AES256 level encryption with SHA256 or SHA2 hashing.

1.53 SECURITY PROCESSES:

The Vendor shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Vendor. For example: virus checking and port sniffing.

1.54 IMPORT AND EXPORT OF DATA:

The State shall have the ability to import or export data piecemeal or in entirety at its discretion without interference from the Vendor. This includes the ability for the State to import or export data to/from other Vendors.

1.55 PASSWORD PROTECTION:

The website(s) and or service(s) that will be hosted by the Vendor for the State will be password protected. If the Vendor provides the user with a preset or default password that password cannot include any Personally Identifiable Information, data protected under the Family Educational Rights and Privacy Act, Protected Health Information, Federal Tax Information or any information defined under state statute as Confidential Information or fragment thereof.

1.56 USE OF PRODUCTION DATA IN A NON-PRODUCTION ENVIRONMENT:

The Vendor cannot use protected State data, whether legally protected or protected by industry standards, in a non-production environment. Any non-production environment that is found to have legally protected production data, must be purged immediately and the State Contact notified. The State will decide if this event is to be considered a security incident. "Legally protected production data" is any data protected under Federal or State Statute or regulation. "Industry standards" are data handling requirements specific to an industry. An example of data protected by industry standards is payment card industry information (PCI). Protected data that is de-identified, aggregated or hashed is no longer considered to be legally protected.

1.57 BANNED SERVICES:

The Vendor warrants that any hardware or hardware components used to provide the services covered by this Agreement were not manufactured by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities. Any company considered to be a security risk by the government of the United States under the International Emergency Economic Powers Act or in a United States appropriation bill will be included in this ban.

1.58 MULTIFACTOR AUTHENTICATION FOR HOSTED SYSTEMS:

If the Vendor is hosting on their system or performing Software as a Service where there is the potential for the Vendor and/or the Vendor's subcontractor to see protected State data, then Multifactor Authentication (MFA) must be used to before this data can be accessed. The Vendor's MFA, at a minimum must adhere to the requirements of *Level 3 Authentication Assurance for MFA* as defined in NIST 800-63.

1.59 SCANNING AUTHORIZATION:

The Consultant will, upon request by the State but no more than once per year, (1) make appropriate personnel available to share and discuss Management Responses of Consultant's most recent annual vulnerability scan report, SOC audit, PCI audit, and HIPAA audit, and (2) with sufficient notice, provide the State with an ephemeral environment to provide safe and secure security scans.

1.60 USE OF ABSTRACTION TECHNOLOGIES:

The Vendor's application must use abstraction technologies in all applications, that is the removal of the network control and forwarding functions that allows the network control to become directly programmable and the underlying infrastructure to be separated for applications and network services.

The Vendor warrants that hard-coded references will not be used in the application. Use of hard-coded references will result in a failure to pass pre-production testing or may cause the application to fail or be shut down at any time without warning and or be removed from production. Correcting the hardcoded references is the responsibility of the Vendor and will not be a project change chargeable to the State. If the use of hard-coded references is discovered after User Acceptance Testing the Vendor will correct the problem at no additional cost.

1.61 APPLICATION PROGRAMMING INTERFACE:

Vendor documentation on application programming interface must include a listing of all data types, functional specifications, a detailed explanation on how to use the Vendor's application programming interface and tutorials. The tutorials must include working sample code.

Attachment C-1
Excepted Entities under Section 1.9.1

- Byrne Technologies
- cloudPWR

Exhibit D – Security Acknowledgement Form

Please return agreement to your BIT Manager or Designated BIT Contact

All BIT employees and Vendors of the State must sign; **Agreement to Comply with BIT Information Technology Security Policy (the "Policy")**. Users are responsible for compliance to all information security policies and procedures. By signature below, the vendor hereby acknowledges and agrees to the following:

1. Vendor uses non-public State of South Dakota technology infrastructure or information;
2. Vendor will protect technology assets of the State from unauthorized activities including disclosure, modification, deletion, and usage;
3. Vendor agrees to follow state and federal regulations in regard to confidentiality and handling of data;
4. Vendor has read and agrees to abide by the Policy;
5. Vendor consents to State contact regarding Policy violations;
6. Vendor shall abide by the policies described as a condition of contract with the state for professional services;
7. Vendor understands that any individual found to violate the Policy is subject to disciplinary action, including but not limited to, privilege revocation, employment termination or financial reimbursement to the State;
8. Access to the technology infrastructure of the State is a privilege which may be changed or revoked at the discretion of BIT management;
9. Access to the technology infrastructure of the State automatically terminates upon contract termination;
10. Vendor shall promptly report violations of security policies to a BIT manager or State Contact and BIT Help Desk (605.773.4357);
11. The Policy may be amended from time to time. The State of South Dakota recommends employees and vendors for the State to regularly review the appropriate Policy and annual amendments.

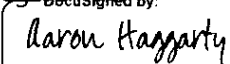
Information Technology Security Policy – BIT: <http://intranet.bit.sd.gov/policies/>

Information Technology Security Policy – CLIENT: <http://intranet.bit.sd.gov/policies/>

Information Technology Security Policy – CONTRACTOR: <http://bit.sd.gov/vendor/default.aspx>

Acknowledgement: State of South Dakota Information Technology Security Policy

Vendor: If the individual is signing for their entire company by signing this form the individual affirms that they have the authority to commit their entire organization and all its employees to follow the terms of this agreement.

<small>DocuSigned by:</small> 	10/1/2021		
<small>A041990928344D8...</small>			
Vendor signature	Date	BIT Manager or Contact	Date